



US006154544A

United States Patent [19]

Farris et al.

[11] **Patent Number:** 6,154,544[45] **Date of Patent:** Nov. 28, 2000[54] **ROLLING CODE SECURITY SYSTEM**[75] **Inventors:** Bradford L. Farris, Chicago; James J. Fitzgibbon, Streamwood, both of Ill.[73] **Assignee:** The Chamberlain Group, Inc., Elmhurst, Ill.[21] **Appl. No.:** 08/873,149[22] **Filed:** Jun. 11, 1997**Related U.S. Application Data**

[63] Continuation of application No. 08/446,886, May 17, 1995, abandoned.

[51] **Int. Cl.⁷** H04L 9/00[52] **U.S. Cl.** 380/262; 340/825.72[58] **Field of Search** 380/23, 28, 48, 380/49, 25, 259, 260, 261, 262, 44; 340/825.72, 825.25, 825.31, 825.69; 341/176

32 44 049 A1	9/1984	Germany .
33 09 802 A1	9/1984	Germany .
3309802 A1	9/1984	Germany .
33 20 721 A1	12/1984	Germany .
33 09 802 C2	7/1985	Germany .
3309802 C2	7/1985	Germany .
3407 436 A1	8/1985	Germany .
3407 469 A1	9/1985	Germany .
3532 156 A1	3/1987	Germany .
36 36 822 C1	10/1987	Germany .
3636822	10/1987	Germany .
89 8225	of 0000	South Africa .
90/4088	5/1990	South Africa .
2 023 899A	1/1980	United Kingdom .
2 051 442	1/1981	United Kingdom .
2 099 195	12/1982	United Kingdom .
2 118 614	11/1983	United Kingdom .
2 131 992	6/1984	United Kingdom .
2 133 073	7/1984	United Kingdom .
2 184 774	7/1987	United Kingdom .
93/20538	10/1993	WIPO .
94/11829	5/1994	WIPO .

OTHER PUBLICATIONSAbrams, and Podell, "Tutorial Computer and Network Security," *District of Columbia: IEEE*, 1987, pp. 1075-1081.

(List continued on next page.)

Primary Examiner—Pinchus M. Laufer*Assistant Examiner*—Ho S. Song*Attorney, Agent, or Firm*—Fitch, Even, Tabin & Flannery[56] **References Cited****U.S. PATENT DOCUMENTS**

Re. 29,525	1/1978	Willmott .
Re. 30,957	6/1982	Feistel .
Re. 35,364	10/1996	Heitschel et al. 364/400
2,405,500	8/1946	Guannella .

(List continued on next page.)

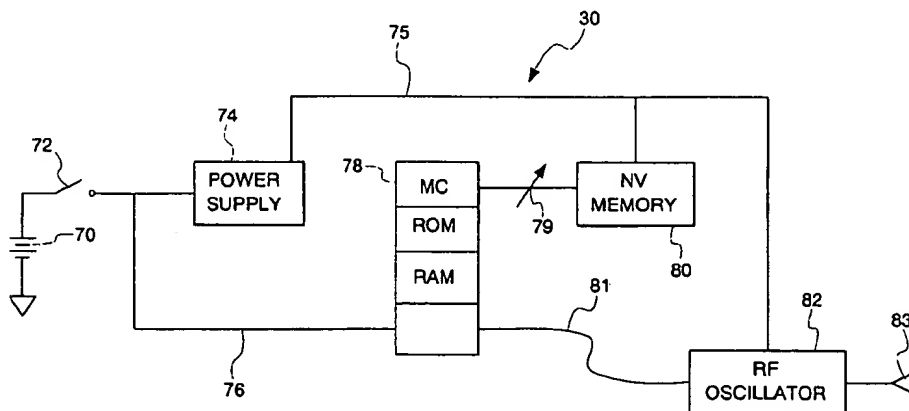
FOREIGN PATENT DOCUMENTS

0 043 270 A1	1/1982	European Pat. Off. .
0 103 790 A2	3/1984	European Pat. Off. .
0 244 322 B1	11/1987	European Pat. Off. .
0 155 378	7/1988	European Pat. Off. .
0 154 019	8/1988	European Pat. Off. .
0 311 112	4/1989	European Pat. Off. .
0 335 912 B1	10/1989	European Pat. Off. .
0 311 112 A2	12/1989	European Pat. Off. .
0 459 781 B1	12/1991	European Pat. Off. .
2 606 232	5/1988	France .
2 607 544	7/1988	France .
2 685 520	6/1993	France .
32 34 538 A1	3/1984	Germany .
32 34 539 A1	3/1984	Germany .

[57] **ABSTRACT**

A rolling code transmitter is useful in a security system for providing secure encrypted RF transmission comprising an interleaved trinary bit fixed code and rolling code. A receiver demodulates the encrypted RF transmission and recovers the fixed code and rolling code. Upon comparison of the fixed and rolling codes with stored codes and determining that the signal has emanated from an authorized transmitter, a signal is generated to actuate an electric motor to open or close a movable barrier.

En/decryption

25 Claims, 16 Drawing Sheets**Microfiche Appendix Included**
(1 Microfiche, 52 Pages)

U.S. PATENT DOCUMENTS

3,716,865	2/1973	Willmott .		4,754,255	6/1988	Sanders et al. .	
3,735,106	5/1973	Hollaway	235/154	4,755,792	7/1988	Pezzolo et al. .	
3,792,446	2/1974	McFiggins et al. .		4,758,835	7/1988	Rathmann et al. .	
3,798,359	3/1974	Feistel .		4,761,808	8/1988	Howard	329/95
3,798,360	3/1974	Feistel .		4,779,090	10/1988	Miczlik et al. .	29/847
3,798,605	3/1974	Feistel .		4,794,268	12/1988	Nakano et al. .	307/10 AT
3,845,277	10/1974	Voss et al. .		4,794,622	12/1988	Isaacman et al. .	375/71
3,890,601	6/1975	Pietrolewicz .		4,796,181	1/1989	Wiedemer .	
3,906,348	9/1975	Willmott .		4,799,061	1/1989	Abraham et al. .	
3,938,091	2/1976	Atalla et al. .		4,800,590	1/1989	Vaughan .	
4,037,201	7/1977	Willmott .		4,802,114	1/1989	Sogame .	
4,064,404	12/1977	Willmott et al. .		4,807,052	2/1989	Amano .	
4,078,152	3/1978	Tuckerman, III .		4,808,995	2/1989	Clark et al. .	
4,138,735	2/1979	Allocca et al. .		4,825,200	4/1989	Evans et al. .	
4,178,549	12/1979	Ledenbach et al. .	325/38 R	4,825,210	4/1989	Bachhuber et al. .	340/825.31
4,195,196	3/1980	Feistel .		4,831,509	5/1989	Jones et al. .	
4,195,200	3/1980	Feistel .		4,835,407	5/1989	Kataoka et al. .	307/105
4,196,310	4/1980	Forman et al. .		4,845,491	7/1989	Fascenda et al. .	
4,218,738	8/1980	Matyas et al. .		4,847,614	7/1989	Keller	340/825.56
4,304,962	12/1981	Fracassi et al. .		4,855,713	8/1989	Brunius .	
4,305,060	12/1981	Apple et al. .	340/825.65	4,856,081	8/1989	Smith .	
4,316,055	2/1982	Feistel .		4,859,990	8/1989	Isaacman	340/539
4,326,098	4/1982	Bouricius et al. .		4,870,400	9/1989	Downs et al. .	340/825.31
4,327,444	4/1982	Court	455/100	4,878,052	10/1989	Schulze .	
4,328,414	5/1982	Atalla .		4,881,148	11/1989	Lambropoulos et al. .	361/172
4,328,540	5/1982	Matsuoka et al. .	364/167	4,885,778	12/1989	Weiss .	
4,380,762	4/1983	Capasso .		4,888,575	12/1989	De Vault	340/426
4,385,296	5/1983	Tsubaki et al. .		4,890,108	12/1989	Drori et al. .	
4,393,269	7/1983	Konheim et al. .		4,905,279	2/1990	Nishio .	
4,418,333	11/1983	Schwarzbach et al. .		4,912,463	3/1990	Li .	
4,426,637	1/1984	Apple et al. .	340/825.65	4,914,696	4/1990	Dudczak et al. .	380/21
4,445,712	5/1984	Smagala-Romanoff .		4,918,690	4/1990	Markkula, Jr. et al. .	370/94
4,447,890	5/1984	Duwel et al. .		4,922,168	5/1990	Waggamon et al. .	
4,454,509	6/1984	Buennagel et al. .		4,922,533	5/1990	Philippe .	
4,464,651	8/1984	Duham	340/521	4,928,098	5/1990	Dannhaeuser .	
4,471,593	9/1984	Schober	455/90	4,931,789	6/1990	Pinnow .	
4,491,774	1/1985	Schmitz	318/282	4,939,792	7/1990	Urbish et al. .	455/347
4,509,093	4/1985	Stellberger	361/172	4,942,393	7/1990	Waraksa et al. .	340/825.72
4,529,980	7/1985	Liotine et al. .		4,951,029	8/1990	Severson .	
4,535,333	8/1985	Twardowski .		4,963,876	10/1990	Sanders	423/300
4,574,247	3/1986	Jacob .		4,979,832	12/1990	Ritter .	
4,578,530	3/1986	Zeidler .		4,980,913	12/1990	Sekret .	
4,581,606	4/1986	Mallory	340/539	4,988,992	1/1991	Heitschel et al. .	
4,590,470	5/1986	Koenig	340/825.31	4,992,783	2/1991	Zdunek et al. .	340/825
4,593,155	6/1986	Hawkins	179/25 A	4,999,622	3/1991	Amano et al. .	
4,596,898	6/1986	Pemmaraju .		5,001,332	3/1991	Schrenk	235/492
4,596,985	6/1986	Bongard et al. .	340/825.69	5,023,908	6/1991	Weiss .	
4,599,489	7/1986	Cargile .		5,049,867	9/1991	Stouffer .	
4,602,357	7/1986	Yang et al. .	367/93	5,055,701	10/1991	Takeuchi	307/10.2
4,611,198	9/1986	Levinson et al. .	340/539	5,058,161	10/1991	Weiss .	
4,623,887	11/1986	Welles, II .		5,060,263	10/1991	Bosen et al. .	
4,626,848	12/1986	Ehlers .		5,103,221	4/1992	Memmola	340/825.31
4,628,315	12/1986	Douglas	340/870.26	5,107,258	4/1992	Soum	340/825.31
4,630,035	12/1986	Stahl et al. .	340/539	5,126,959	6/1992	Kurihara	364/717
4,633,247	12/1986	Hegeler .		5,144,667	9/1992	Pogue, Jr. et al. .	
4,638,433	1/1987	Schindler	364/400	5,146,067	9/1992	Sloan et al. .	235/381
4,646,080	2/1987	Genest et al. .	340/825.31	5,148,159	9/1992	Clark et al. .	
4,652,860	3/1987	Weishaupt et al. .	340/539	5,153,581	10/1992	Hazard	340/825
4,670,746	6/1987	Taniguchi et al. .	340/825.31	5,159,329	10/1992	Lindmayer et al. .	340/825.72
4,686,529	8/1987	Kleefeldt	341/825.69	5,168,520	12/1992	Weiss .	
4,695,839	9/1987	Barbu et al. .		5,193,210	3/1993	Nicholas et al. .	
4,703,359	10/1987	Rumbolt et al. .		5,224,163	6/1993	Gasser et al. .	
4,710,613	12/1987	Shigenaga .		5,237,614	8/1993	Weiss .	
4,716,301	12/1987	Willmott et al. .		5,252,960	10/1993	Duham ..	
4,720,860	1/1988	Weiss .		5,278,907	1/1994	Snyder et al. .	380/48
4,723,121	2/1988	van den Boom et al. .	340/825.31	5,361,062	11/1994	Weiss et al. .	
4,731,575	3/1988	Sloan	324/113	5,363,448	11/1994	Koopman, Jr. et al. .	
4,737,770	4/1988	Brunius et al. .		5,365,225	11/1994	Bachhuber	340/825.31
4,740,792	4/1988	Sagey et al. .	342/457	5,367,572	11/1994	Weiss .	
4,750,118	6/1988	Heitschel et al. .		5,369,706	11/1994	Latka	380/23
				5,412,379	5/1995	Waraksa et al. .	
				5,414,418	5/1995	Audros, Jr. .	

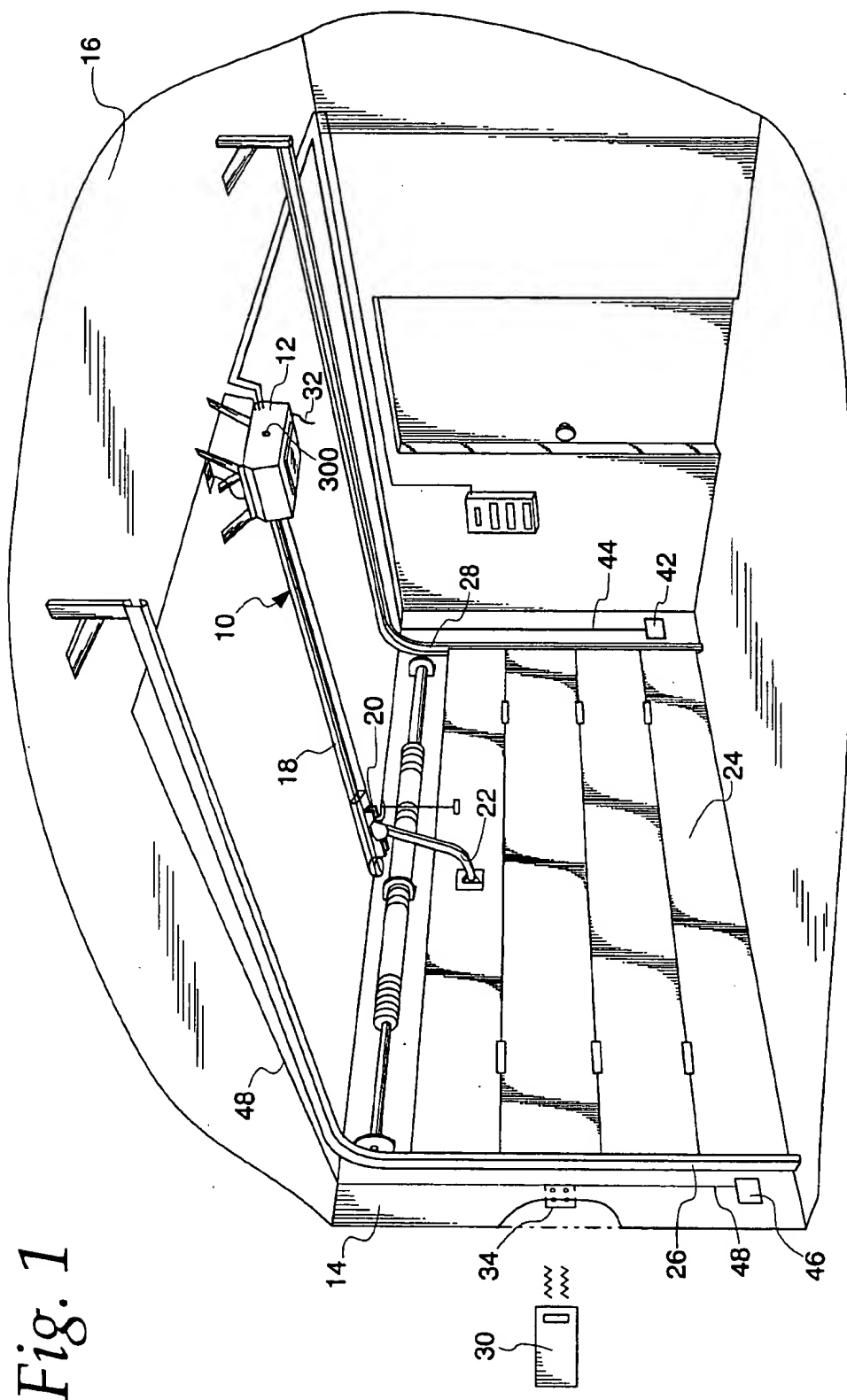
5,420,925	5/1995	Michaels	380/23
5,442,341	8/1995	Lambropoulos .	
5,471,668	11/1995	Soenen et al. .	
5,473,318	12/1995	Martel .	
5,479,512	12/1995	Weiss .	
5,485,519	1/1996	Weiss .	
5,517,187	5/1996	Bruwer et al.	340/825.3
5,598,475	1/1997	Soenen et al. .	
5,657,388	8/1997	Weiss .	
5,686,904	11/1997	Bruwer .	
5,778,348	7/1998	Manduley et al. .	
5,898,397	4/1999	Murray	341/176

OTHER PUBLICATIONS

- Bruwer, Frederick J. "Die Toepassing Van Gekombineerde Konvolusiekodering en Modulasie op HF-Datakommunikasie," District of Pretoria in South Africa Jul. 1998.
- Davies, D.W. and Price, W.C. "Security for Computer Networks," John Wiley and Sons, 1984. Chapter 7, pp 175-176.
- Davies, Donald W., "Tutorial: The Security of Data in Networks," pp. 13-17, *New York: IEEE*, 1981.
- Diffie and Hellman, Exhaustive Cryptanalysis of the NBS Data Encryption Standard, pp. 74-84, *Computer*, Jun. 1977.
- Diffie and Hellman. "Privacy and Authentication: An Introduction to Cryptography," pp. 29-33, *Proceedings of the IEEE* 67(3), Mar. 1979.
- Feistel, H., "Cryptography and Computer Privacy," pp. 15-23, *Scientific American*, May 1973.
- Fenzl, H. and Kliner, A., "Electronic Lock System: Convenient and Safe," pp. 150-153, *Siemens Components XXI*, No. 4, 1987.
- Greenlee, B.M., "Requirements for Key Management Protocols in the Wholesale Financial Services Industry," pp. 22-28, *IEEE Communications Magazine*, Sep. 1985.
- ISO 8732: 1988(E): Banking Key Management (Wholesale) Annex D: Windows and Windows Management, Nov. 1988.
- Konheim, A.G., *Cryptography: A Primer*, pp. 285-347, New York: John Wiley, 1981.
- Ruffell, J. "Battery Low Indicator," p. 59, *Electron Electronics* 15-165, Mar. 1989.
- Seberry, J. and Pieprzyk, *Cryptography—An Introduction to Computer Security*, Prentice Hall of Australia, YTY LTD, 1989. pp. 134-136.
- Welsh, Dominic, *Codes and Cryptography*, pp. 7.0-7.1 Clarendon Press, 1988.
- Abramson, Norman. "The Aloha System—Another alternative for computer communications," pp. 281-285, University of Hawaii, 1970.
- "Access Transmitters—Access Security System", pp. 1-2, Undated. <http://www.webercreations.com/access/security.html>.
- Alexi, Werner, et al. "RSA and Rabin Functions: Certain Parts Are As Hard As The Whole", pp. 194-209, *Siam Computing*, vol. 14, No. 2, Apr. 1988.
- Allianz: Allianz-Zentrum for Technik GmbH—"Detailed requirements for fulfilling the specification profile for electronically coded OEM immobilizers", Issue 22, Jun. 1994 (Translation Jul. 5, 1994).
- Anderson, Ross. "Searching for the Optimum Correlation Attack", pp. 136-143, Computer Laboratory, Pembroke Street, Cambridge CB2 3QG, Undated.
- Baran, P. Distribution Communications, vol. 9, "Security Secrecy and Tamper-free Communications", Rand Corporation, 1964.
- Barbaroux, Paul. "Uniform Results in Polynomial-Time Security", pp. 297-306, *Advances in Cryptology—Eurocrypt 92*, 1992.
- Bellovin, S.M. "Security Problems in the TCP/IP Protocol Suite", pp. 32-49, *Computer Communication Review*, New Jersey, Undated.
- Beutelspacher, Albrecht. *Advances in Cryptology—Eurocrypt 87: "Perfect and Essentially Perfect Authentication Schemes"* (Extended Abstract), pp. 167-170, Federal Republic of Germany, Undated.
- Bloch, Gilbert. "Enigma Before Ultra Polish Work and The French Contribution", 11(3): 142-155, *Cryptologia*, Jul. 1987.
- Brickell, Ernest F. and Stinson, Doug. "Authentication Codes With Multiple Arbiters", pp. 51-55, *Proceedings of Eurocrypt 88*, 1988.
- Burmeister, Mike. "A Remark on the Efficiency of Identification Schemes", pp. 493-495, *Advances in Cryptology—Eurocrypt 90*, 1990.
- Cerf, Vinton G. and Kahn, Robert E. "A Protocol for Packet Network Intercommunication", pp. 637-648, *Transactions on Communications*, vol. Com-22, No. 5, May 1974.
- Cerf, Vinton G. "Issues In Packet-Network Interconnection", pp. 1386-1408, *Proceedings of the IEEE*, 66(11), Nov. 1978.
- Coppersmith, Don. "Fast Evaluation of Logarithms in Fields of Characteristic Two", IT-30(4): pp. 587-594, *IEEE Transactions on Information Theory*, Jul. 1984.
- Davis, Gregory and Palmer, Morris. "Self-Programming, Rolling-Code Technology Creates Nearly Unbreakable RF Security", *Technological Horizons*, Texas Instruments, Inc. (ECN), Oct. 1996.
- Deavours, Cipher A., et al. "Analysis of the Hebern cryptograph Using Isomorphs", pp. 246-261, *Cryptology: Yesterday, Today and Tomorrow*, vol. 1, No. 2, Apr. 1977.
- Deavours, C.A. and Reeds, James. "The Enigma, Part 1, Historical Perspectives", 381-391, *Cryptologia*, 1(4): Oct. 1977.
- Deavours, C.A. and Kruh, L. "The Swedish HC-9 Ciphering Machine", 251-285, *Cryptologia*, 13(3): Jul. 1989.
- Denning, Dorothy E. "Cryptographic Techniques", pp. 135-154, *Cryptography and Data Security*, 1982. Chapter 3.
- Denning, Dorothy E. "A Lattice Model of Secure Information Flow", pp. 236-238, 240, 242, *Communications of the ACM*, vol. 19, No. 5, May 1976.
- De Soete, Marijke. "Some Constructions for Authentication-Secrecy Codes", pp. 57-75, *Advances in Cryptology—Eurocrypt 88*, Undated.
- Diffie, Whitfield and Hellman, Martin E. "New Directions in Cryptography", pp. 644-654, *IEEE, Transactions on Information Theory*, vol. IT-22, No. 6, Nov. 1976.
- Diffie, Whitfield and Hellman, Martin, E. "An RSA Laboratories Technical Note", Version 1.4, Revised Nov. 1, 1993.
- Dijkstra, E.W. "Co-Operating Sequential Processes", pp. 43-112, *Programming Languages*, F. Genuys, NY, Undated.
- Dijkstra, E.W. "Hierarchical Ordering of Sequential Processes", pp. 115-138, *Acta Informatica* 1: 115-138, 1971.
- ElGamal, Taher. "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", pp. 469-472, *IEEE, Transactions on Information Theory*, vol. IT-31, No. 4, Jul. 1985.
- ElGamal, Taher. "A Subexponential Time Algorithm for Computing Discrete Logarithms", pp. 473-481, *IEEE, Transactions on Information Theory*, vol. IT-31, No. 4, Jul. 1985.

- Feistel, Horst, Notz, Wm. A. and Smith, J. Lynn. "Some Cryptographic Techniques for Machine-to-Machine Data Communications", pp. 1545-1554, *Proceedings of the IEEE*, vol. 63, No. 11, Nov. 1975.
- Feistel, Horst. "Cryptography and Computer Privacy", pp. 15-23, *Scientific American*, vol. 228, No. 5, May 1973.
- Fischer, Elliot. "Uncaging the Hagelin Cryptograph", pp. 89-92, *Cryptologia*, vol. 7, No. 1, Jan. 1983.
- Godlewski, Ph. and Camion P. "Manipulations and Errors, Detection and Localization," pp. 97-106, *Proceedings of Eurocrypt 88*, 1988.
- Guillou, Louis C. "Smart Cards and Conditional Access", pp. 481-489, *Proceedings of Eurocrypt*, 1984.
- Guillou, Louis C. and Quisquater, Jean-Jacques. "A Practical Zero-Knowledge Protocol Fitted to Security Micro-processor Minimizing Both Transmission and Memory", pp. 123-128, *Advances in Cryptology—Eurocrypt 88*, 1988.
- Habermann, A. Nico, "Synchronization of Communicating Processes", pp. 171-176, *Communications*, Mar., 1972.
- Hagelin C-35/C-36 (The), (1 page) Undated. <http://hem.p-assagen.se/tan01/C-35.HTML>.
- Jones, Anita K. "Protection Mechanisms and The Enforcement of Security Policies", pp. 228-251, Carnegie-Mellon University, Pittsburgh, PA, 1978.
- Jueneman, R.R. et al. "Message Authentication", pp. 29-40, *IEEE Communications Magazine*, vol. 23, No. 9, Sep. 1985.
- Kahn, Robert E. "The Organization of Computer Resources Into A Packet Radio Network", pp. 177-186, *National Computer Conference*, 1975.
- Kent, Stephen T. "Encryption-Based Protection Protocols for Interactive User-Computer Communication", pp. 1-121, (See pp. 50-53) May 1976.
- Kent, Stephen T. "Protocol Design Considerations for Network Security", pp. 239-259, *Proc. NATO Advanced Study Institute on Interlinking of Computer Networks*, 1979.
- Kent, Stephen T. "A comparison of some aspects of public-key and conventional cryptosystems", pp. 4.3.1-5, *ICC '79 Int. Conf. on Communications*; Boston, MA, Jun. 1979.
- Kent, Stephen T. et al. "Personal authentication system for access control to the Defense Data Network", pp. 89-93, *Conf. Record of Eascon 82 15th Ann Electronics & Aerospace Systems Conf.*; Washington, DC; Sep. 1982.
- Kent, Stephen T. "Security requirements and protocols for a broadcast scenario", vol. com-29, No. 6, pp. 778-786, *IEEE Transactions on Communications*, Jun. 1981.
- Kent, Stephen T. "Comments on 'security problems in the TCP/IP protocol suite'", *Computer Communication Review*, vol. 19, Part 3, pp. 10-19, Jul. 1989.
- Kruh, Louis. "How To Use The German Enigma Cipher Machine: A Photographic Essay", pp. 291-296, *Cryptologia*, vol. No. 7, No. 4, Oct. 1983.
- Kruh, Louis. "Devices and Machines: The Hagelin Cryptographer, Type C-52", *Cryptologia*, vol. 3, No. 2, Apr. 1979.
- Kuhn, G.J. "Algorithms for Self-Synchronizing Ciphers" *Comsig 88*, University of Pretoria, Pretoria, pp. 159-164, 1988.
- Kuhn, G.J. et al. "A Versatile High-Speed Encryption Chip", (Presented at the INFOSEC '90 Symposium, Pretoria), Mar. 16, 1990.
- Lamport, Leslie. "The Synchronization of Independent Processes", pp. 15-34, *Acta Informatica*, vol. 7, 1976.
- Linn, John and Kent, Stephen T. "Electronic Mail Privacy Enhancement", pp. 40-43, *American Institute of Aeronautics and Astronautics, Inc.*, 1986.
- Lloyd, Sheelagh. "Counting Functions Satisfying A Higher Order Strict Avalanche Criterion", pp. 63-74, 1990.
- Massey, James L. "The Difficulty With Difficulty" (4 pages), Undated. <http://www.iacr.org/conferences/ec96/massey/html/framesmassey.html>.
- McIvor, Robert. "Smart Cards" pp. 152-159, *Scientific American*, vol. 253, No. 5, Nov. 1985.
- Meier, Willi. "Fast Correlation Attacks on Stream Ciphers", (Extended Abstract), pp. 301-314, *Eurocrypt 88, IEEE*, 1988.
- Meyer, Carl H. and Matyas, Stephen H., *Cryptography: A New Dimension in Computer Data Security*, pp. 237-249, 1982.
- Michener, J.R. The 'Generalized Rotor' Cryptographic Operator and Some of Its Applications, pp. 97-113, *Cryptologia*, vol. 9, No. 2, Apr. 1985.
- Morris, Robert. "The Hagelin Cipher Machine (M-209): Reconstruction of the Internal Settings", 2(3): pp. 267-289, *Cryptologia*, Jul. 1978.
- Newman, David B., Jr. et al., "Public Key Management for Network Security", pp. 11-16, *IEEE Network Magazine*, 1987.
- "News: Key system for security", p. 68, Apr. 1982.
- Niederreiter, Harald. "Keystream Sequences with a Good Linear Complexity Profile for Every Starting Point", pp. 523-532, *Proceedings of Eurocrypt 89*, 1989.
- Otway, Dave and Rees, Owen. "Efficient and Timely Mutual Authentication", pp. 8-11, Undated.
- Peyret, Patrice et al. "Smart Cards Provide Very High Security and Flexibility in Subscribers Management", 744-752, *IEEE Transactions on Consumer Electronics*, 36(3): Aug. 1990.
- Postel, Jonathan B. et al., "The ARPA Internet Protocol", pp. 261-271, 1981.
- Postel, J. ed. "DOD Standard Transmission Control Protocol", pp. 52-133, Jan. 1980.
- Reed, David P. and Kanodia, Rajendra K. "Synchronization With Eventcounts and Sequencers", vol. 22, No. 2, pp. 115-123, *Communications of the ACM*, Feb. 1979.
- Reynolds, J. and J. Postel. "Official ARPA-Internet Protocols", *Network Working Groups*, Apr. 1985.
- Saab Anti-Theft System: "Saab's Engine Immobilizing Anti-Theft System is a Road-Block for 'Code-Grabbing' Thieves", pp. 1-2, Undated. <http://www.saabusa.com/news/newsindex/alarm.html>.
- Savage, J.E. "Some Simple Self-Synchronizing Digital Data Scramblers", pp. 449-487, *The Bell System Tech. Journal*, Feb. 1967.
- "Secure Terminal Interface Module for Smart Card Applications", *IBM: Technical Disclosure Bulletin*, vol. 28, No. 4, pp. 1488-1489, Sep. 1985.
- Shamir, Adi. "Embedding Cryptographic Trapdoors In Arbitrary Knapsack Systems", pp. 77-79, *Information Processing Letters*, 1983.
- Siegenthaler, T. "Decrypting a Class of Stream Ciphers Using Ciphertext Only", vol. C-34, No. 1, pp. 81-85, *IEEE Transactions on Computers*, Jan. 1985.
- Simmons, Gustavus J. "Message Authentication With Arbitration of Transmitter/Receiver Disputes", pp. 151-165, 1987.
- Smith, J.L. The Design of Lucifer: A Cryptographic Device for Data Communications, pp. 1-65, Apr. 15, 1971.
- Smith, J.L. et al. "An Experimental Application of Cryptography to A Remotely Accessed Data System", *Proceedings of the ACM*, pp. 282-297, Aug. 1972.

- Svigals, J. "Limiting Access to Data in an Identification Card Having A Micro-Processor", *IBM: Technical Disclosure Bulletin*, vol. 27, No. 1B, pp. 580-581, Jun. 1984.
- "Transaction Completion Code Based on Digital Signatures", *IBM: Technical Disclosure Bulletin*, vol. 28, No. 3, pp. 1109-1122, Aug. 1985.
- Turn, Rein. "Privacy Transformations for Databank Systems", pp. 589-601, *National Computer Conference*, 1973.
- Voydock, Victor L. and Kent, Stephen T. "Security Mechanisms in High-Level Network Protocols", *Computing Surveys*, pp. 135-171, vol. 15, No. 2, Jun. 1983.
- Voydock, Victor L. and Kent, Stephen T. "Security in High-Level Network Protocols", *IEEE Communications Magazine*, pp. 12-25, vol. 23, No. 7, Jul. 1985.
- Voydock, Victor L. and Kent, Stephen T. "Security Mechanisms in a Transport Layer Protocol", *Computers & Security*, 325-341, 1985.
- Weinstein, S.B. "Smart credit cards: the answer to cashless shopping", *IEEE Spectrum*, pp. 43-49, Feb. 1984.
- Weissman, C. "Security controls in the ADEPT-50 time-sharing system", *AFIPS Full Joint Computer Conference*, pp. 119-133, 1969.
- Kobus Marneweck, *Guidelines for Keeloq® Secure Learning Implementation*, TB007, 1987 Microchip Technology, Inc., 1-5.
- Chris R., Burger, *Secure Learning RKE Systems Using Keeloq® Encoders*, TB001, 1996 Microchip Technology, Inc., 1-7.
- Keeloq® Code Hopping Encoder, HCS300*, 1996 Microchip Technology, Inc., 1-20.
- Steven Dawson, *Keeloq® Code Hopping Decoder Using Secure Learn*, AN662, 1997 Microchip Technology, Inc., 1-16.
- Keeloq® Code Hopping Decoder, HCS500*, 1997 Microchip Technology, Inc., 1-25.
- Keeloq® NTQ 105 Code Hopping Encoder*, Nanoteq (Pty.) Ltd., Jul. 1993, 1-8.
- Keeloq® NTQ 125D Code Hopping Decoder*, Nanoteq (Pty.) Ltd., Jul. 1993, 1-8.
- Keeloq® NTQ 115 Code Hopping Encoder*, Nanoteq (Pty.) Ltd., Jul. 1993, 1-8.
- Keeloq® NTQ 129D Code Hopping Decoder*, Nanoteq (Pty.) Ltd., Jul. 1993, 1-9.
- G. Davis, *Marcstar™ TRC1300 and TRC1315 Remote Control Transmitter/Receiver*, Texas Instruments, Sep. 12, 1994, 1-24.
- NM95HS01/NM95HS02 HiSeC™ (High Security Code) Generator*, National Semiconductor, Jan. 1995, 1-19.
- Charles Watts, *How to Program the HiSeC™ Remote Keyless Entry Rolling Code Generator*, National Semiconductor, Oct. 1994, 1-14.
- MM57HS01 HiSeC™ Fixed and Rolling Code Decoder*, National Semiconductor, Nov. 11, 1994, 1-8.
- Charles Watts and Jon Harper, *How to Design a HiSeC™ Transmitter*, National Semiconductor, Oct. 1994, 1-4.
- Whitfield Diffie and Martin E. Hellman, Privacy and Authentication: An Introduction to Cryptography, *Proceedings of the IEEE*, vol. 67, No. 3, Mar. 1979, 397-427.
- Benjamin Arazi, Vehicular Implementations of Public Key Cryptographic Techniques, *IEEE Transactions on Vehicular Technology*, vol. 40, No. 3, Aug. 1991, 646-653.
- Ben Davis and Ron DeLong, Combined Remote Key Control and Immobilization System for Vehicle Security, *Power Electronics in Transportation*, IEEE Catalogue No. 96TH8184, Oct. 24, 1996, 125-132.
- Doug Conner, Cryptographic Techniques—Secure Your Wireless Designs, *EDN (Design Feature)*, Jan. 18, 1996, 57-68.
- Maurizio Fragano, Solid State Key/Lock Security System, *IEEE Transactions on Consumer Electronics*, vol. CE-30, No. 4, Nov. 1984, 604-607.



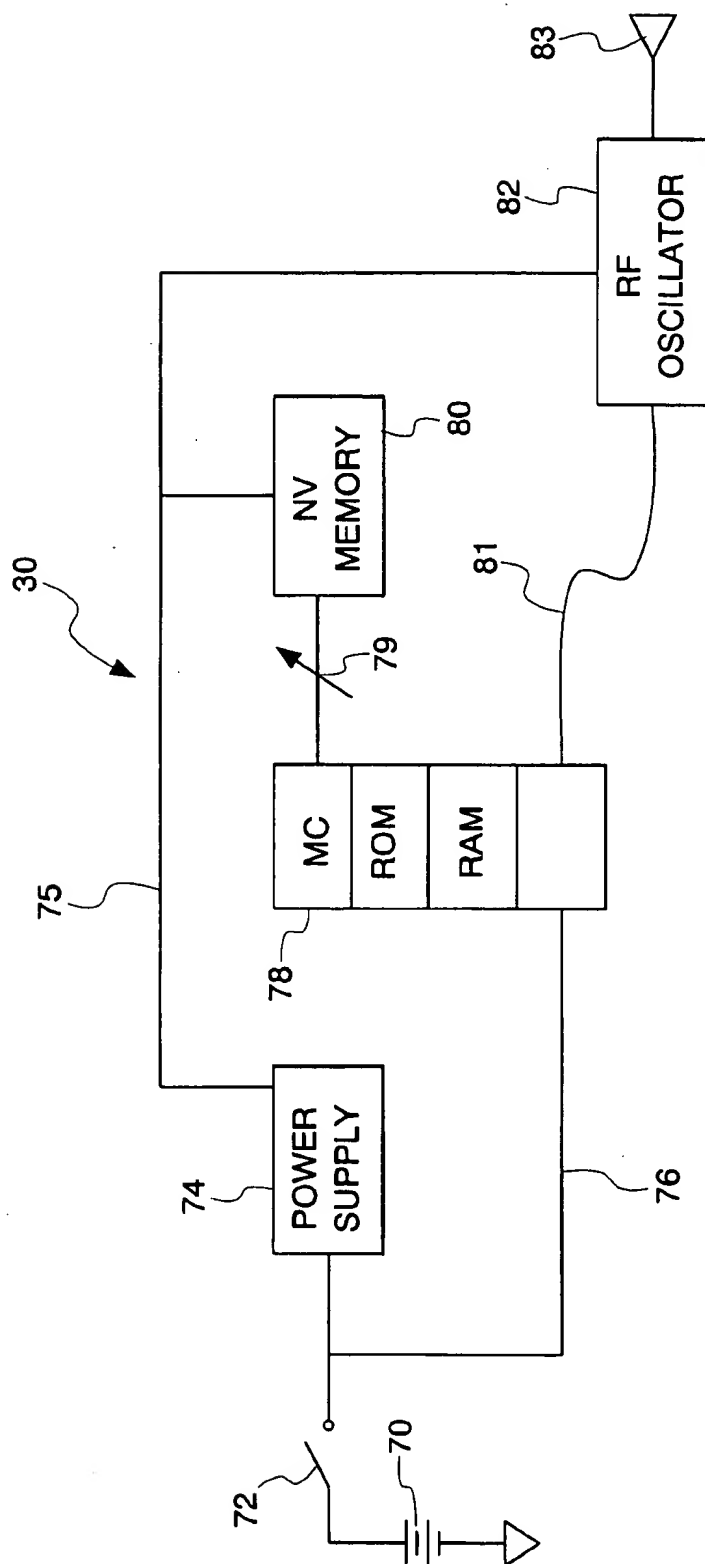


Fig. 2

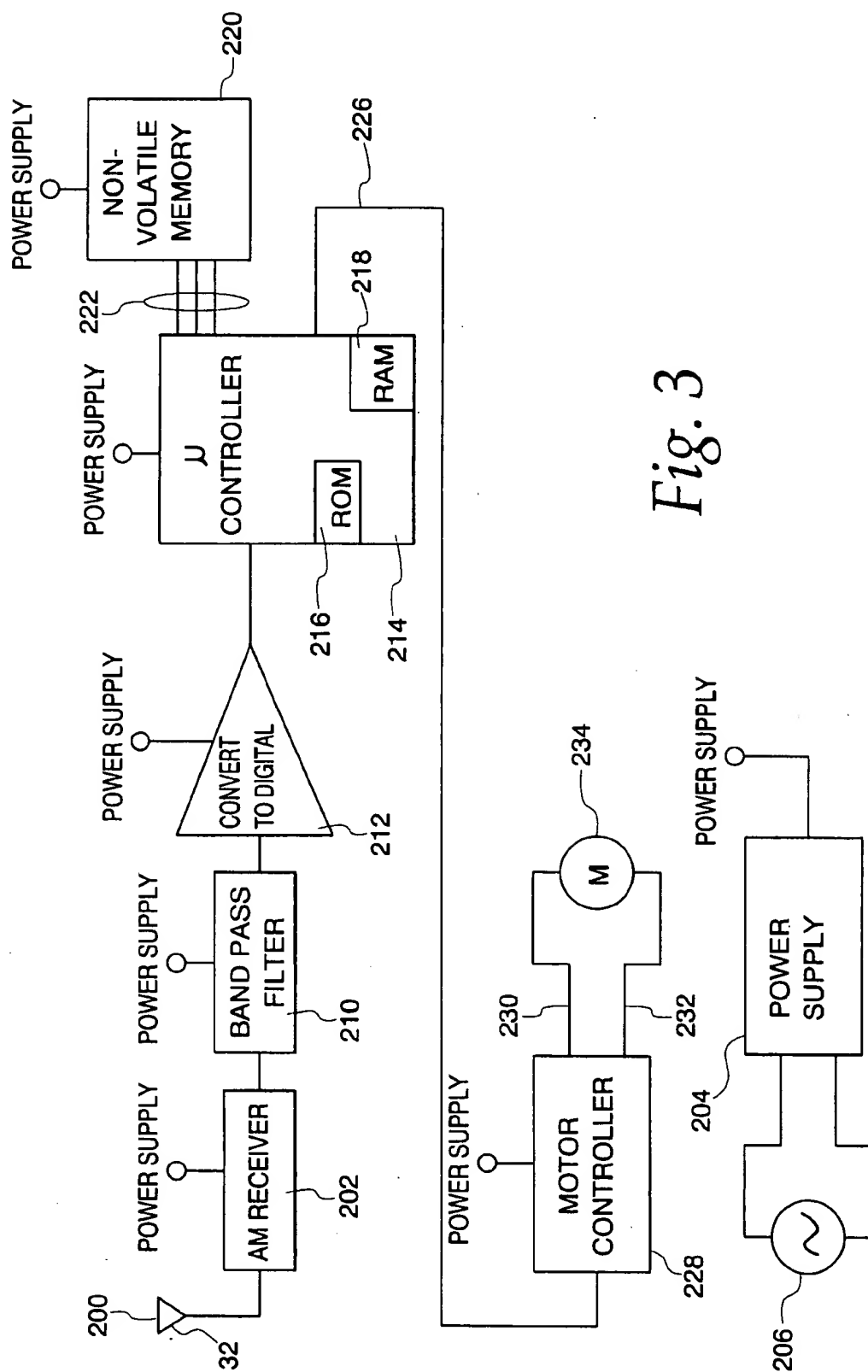


Fig. 3

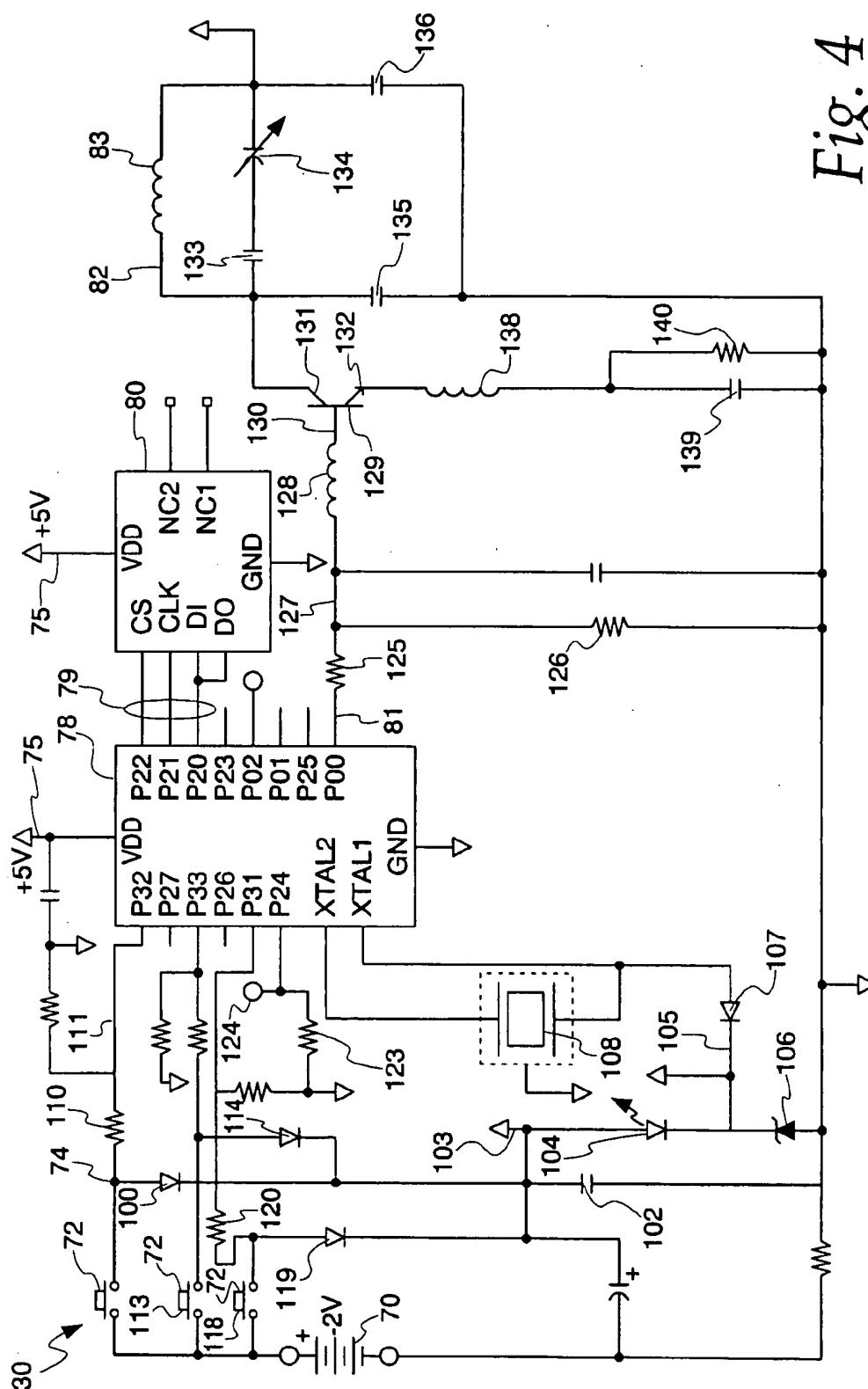
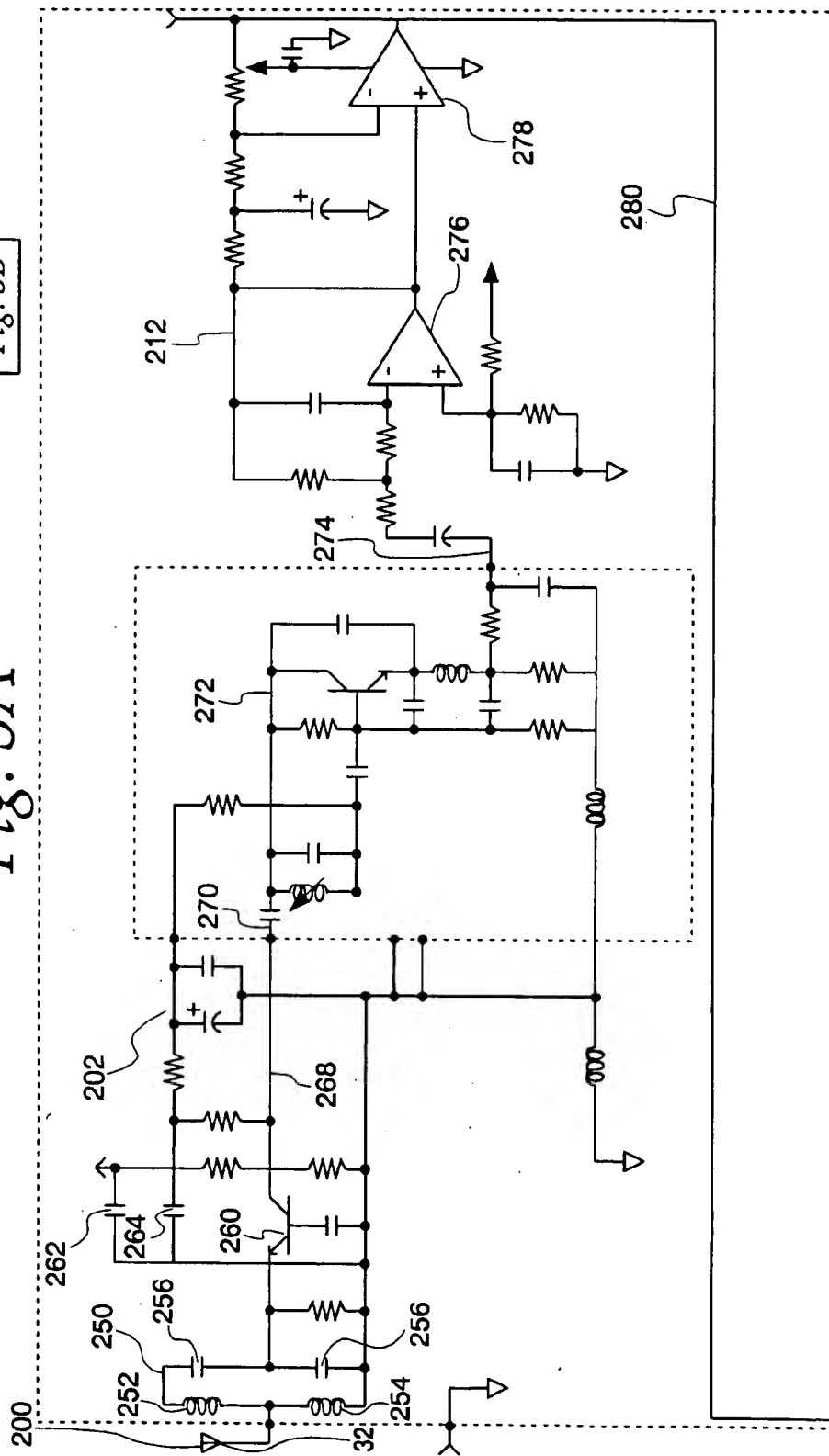
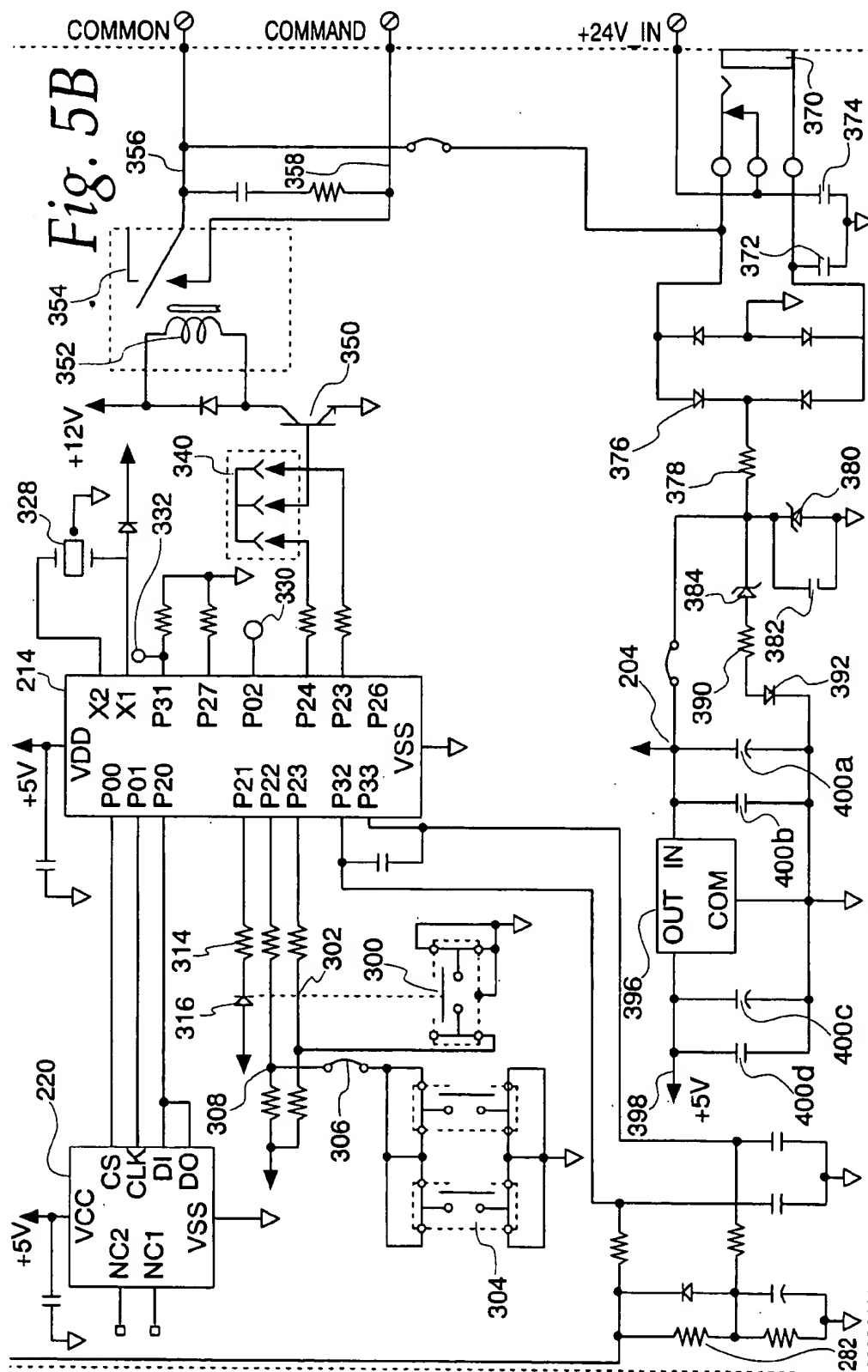


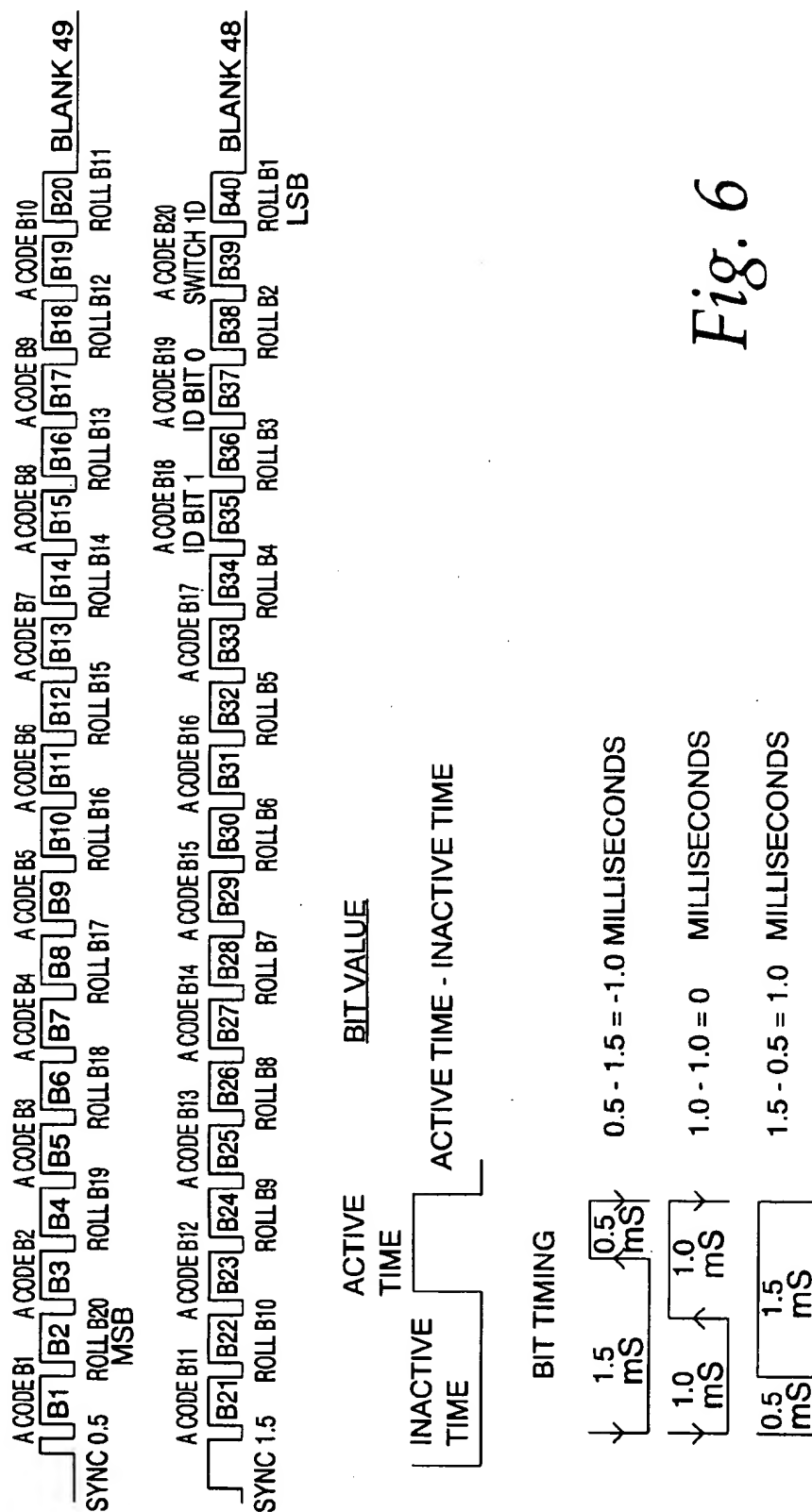
Fig. 4

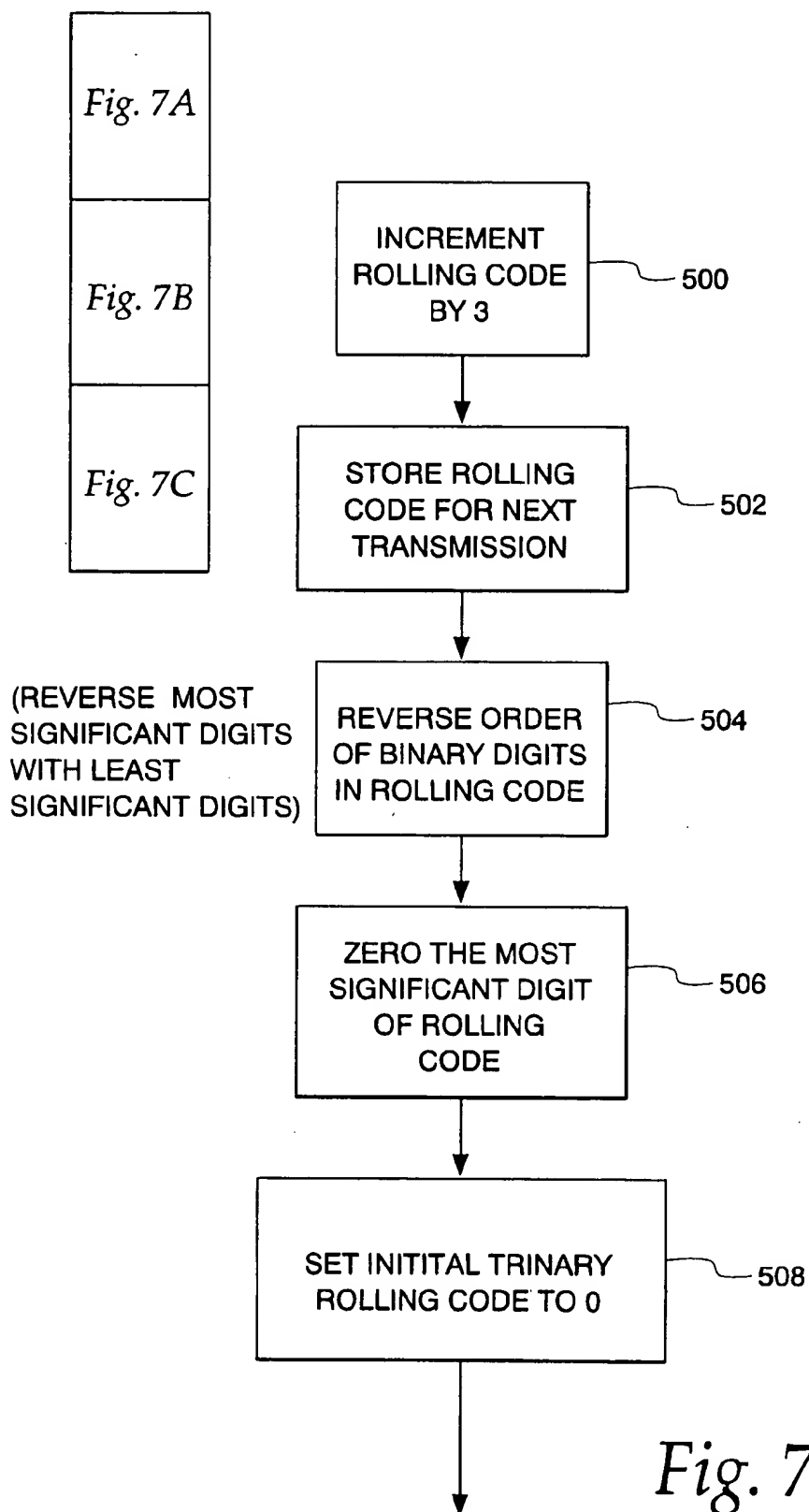
Fig. 5A
Fig. 5B

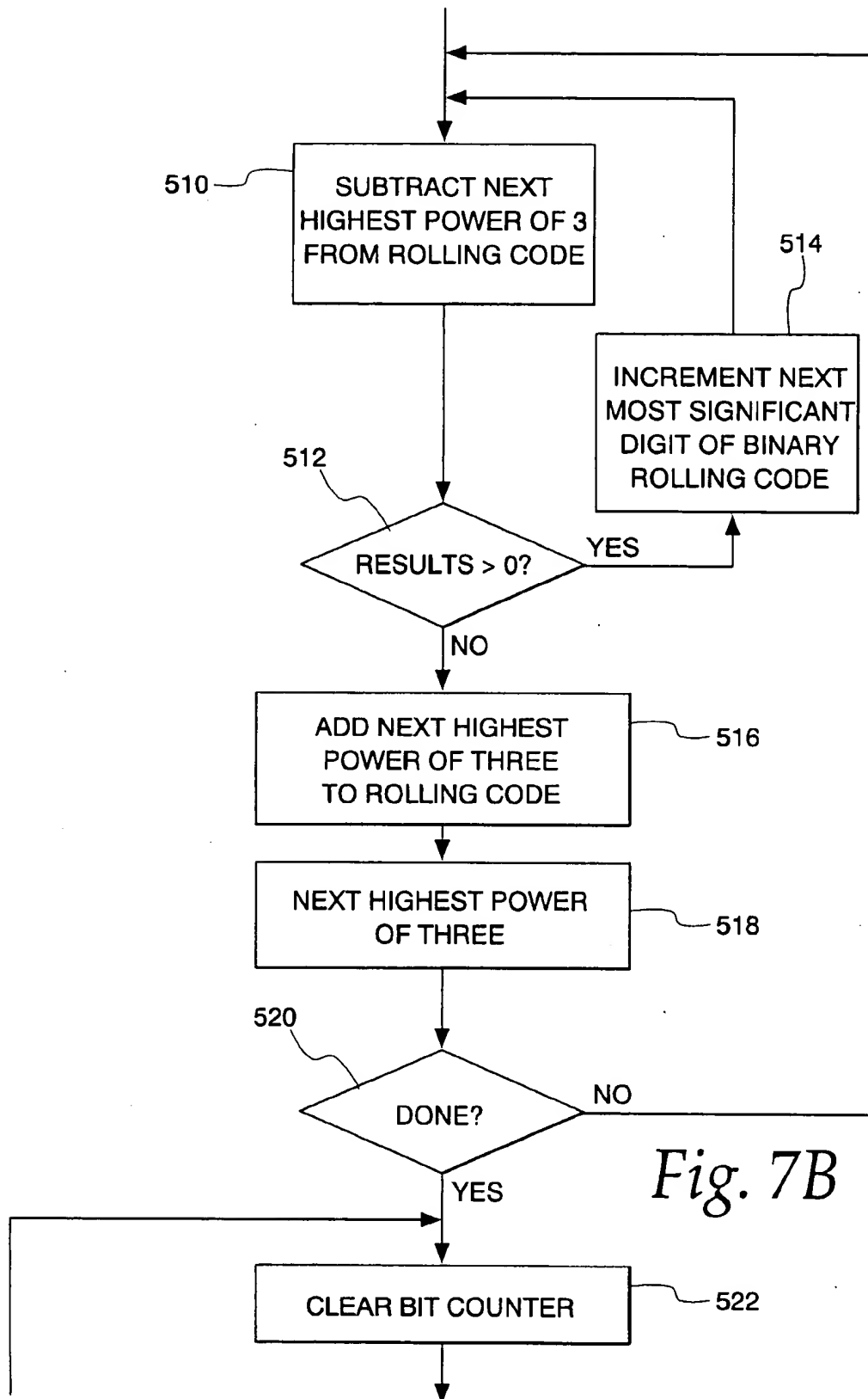
Fig. 5A

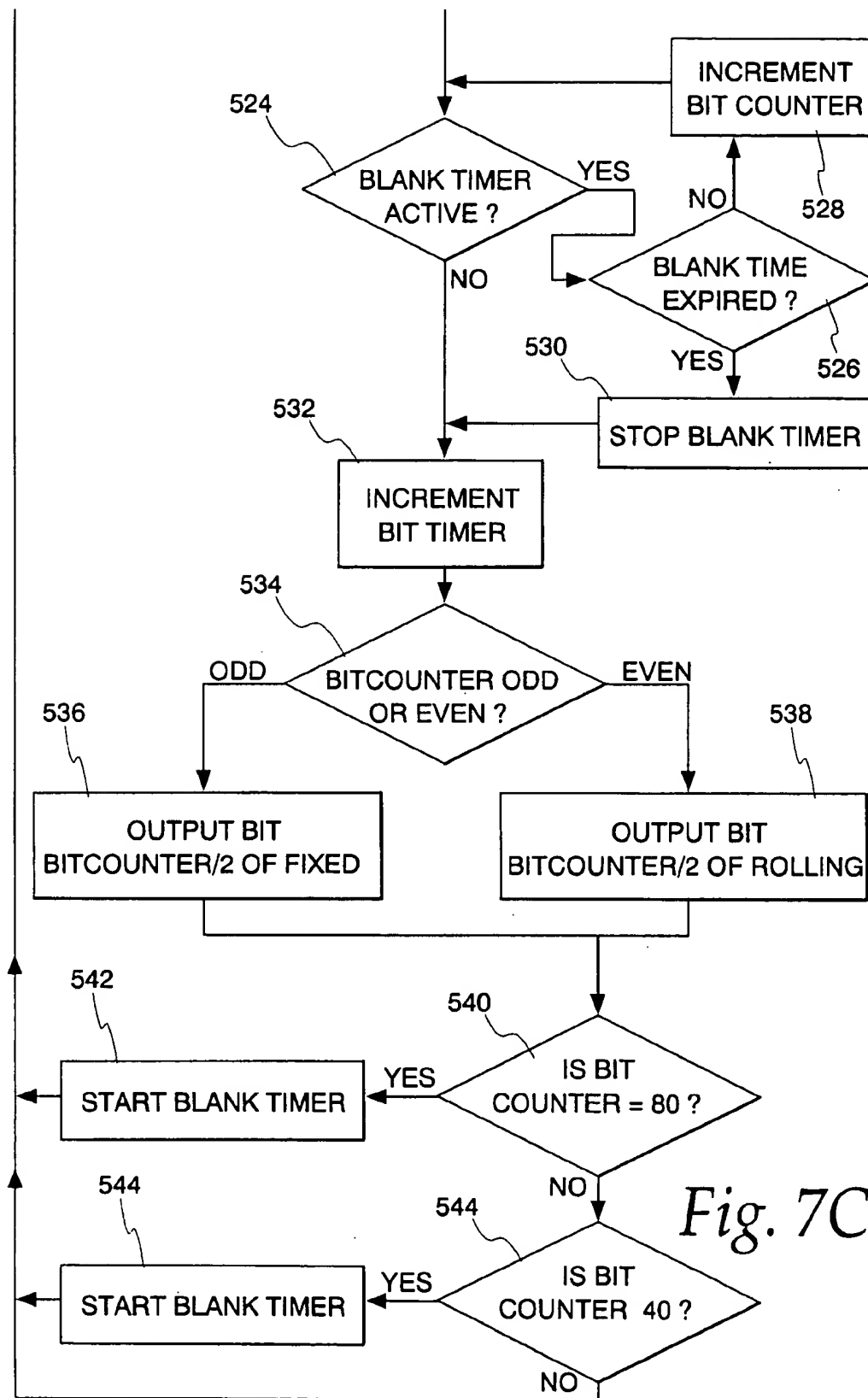


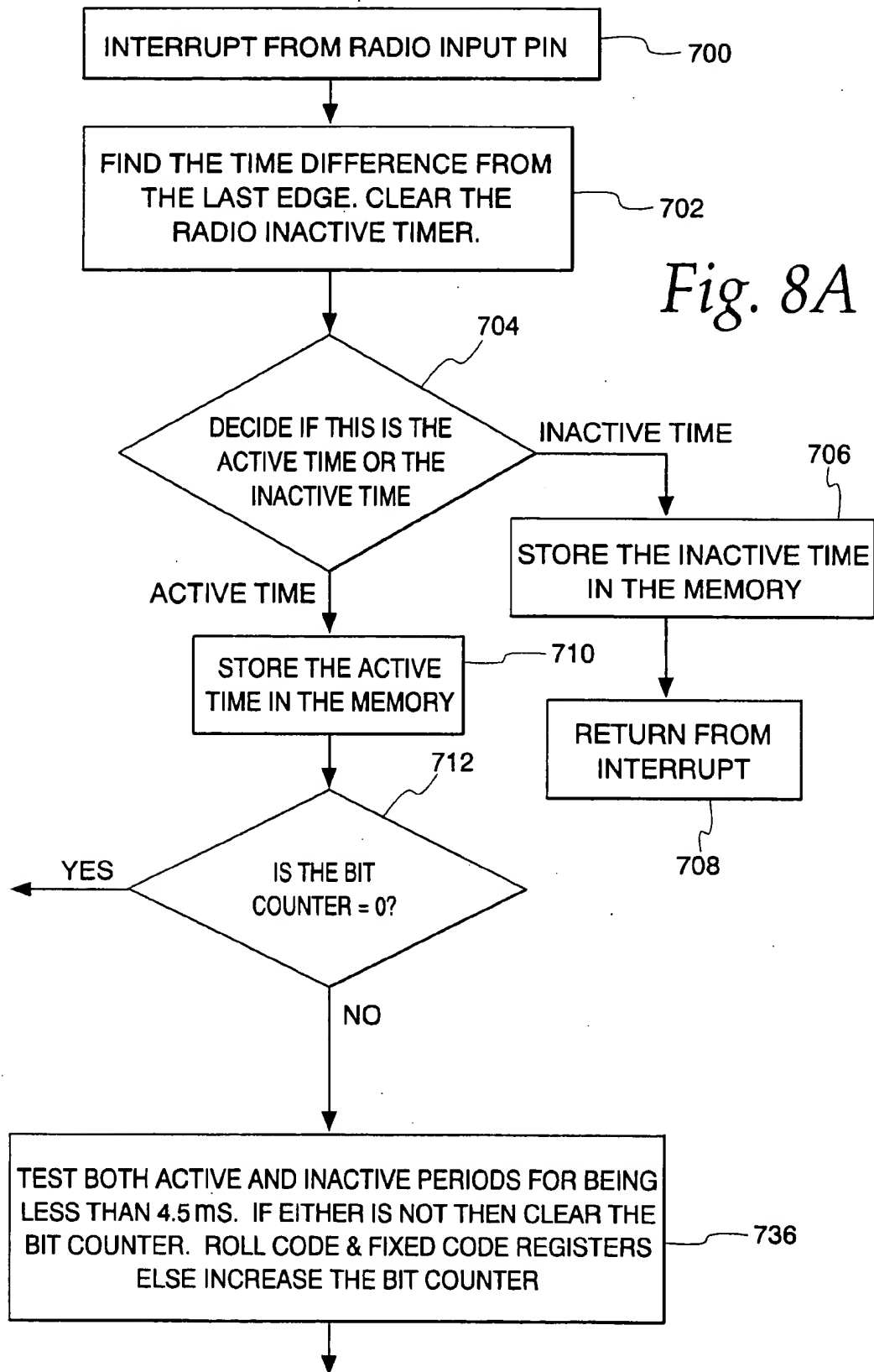


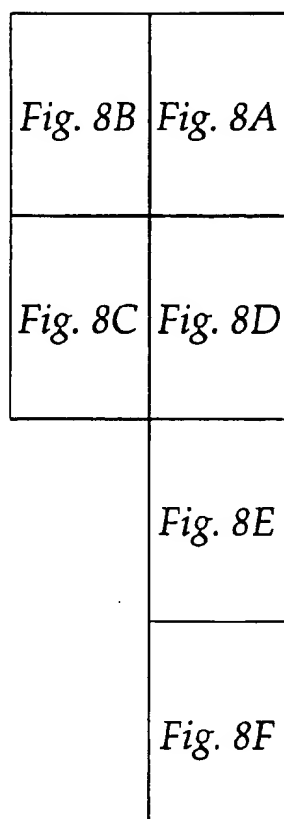
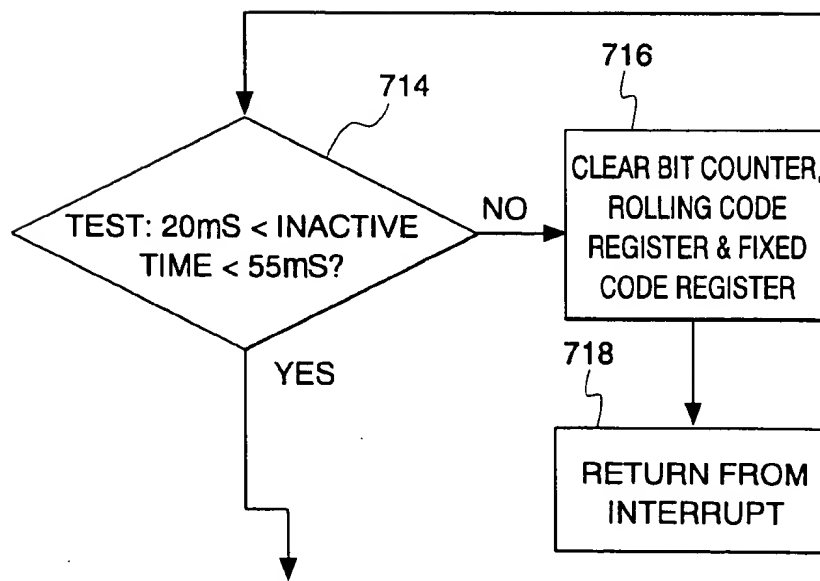




*Fig. 7B*

*Fig. 7C*



*Fig. 8B*

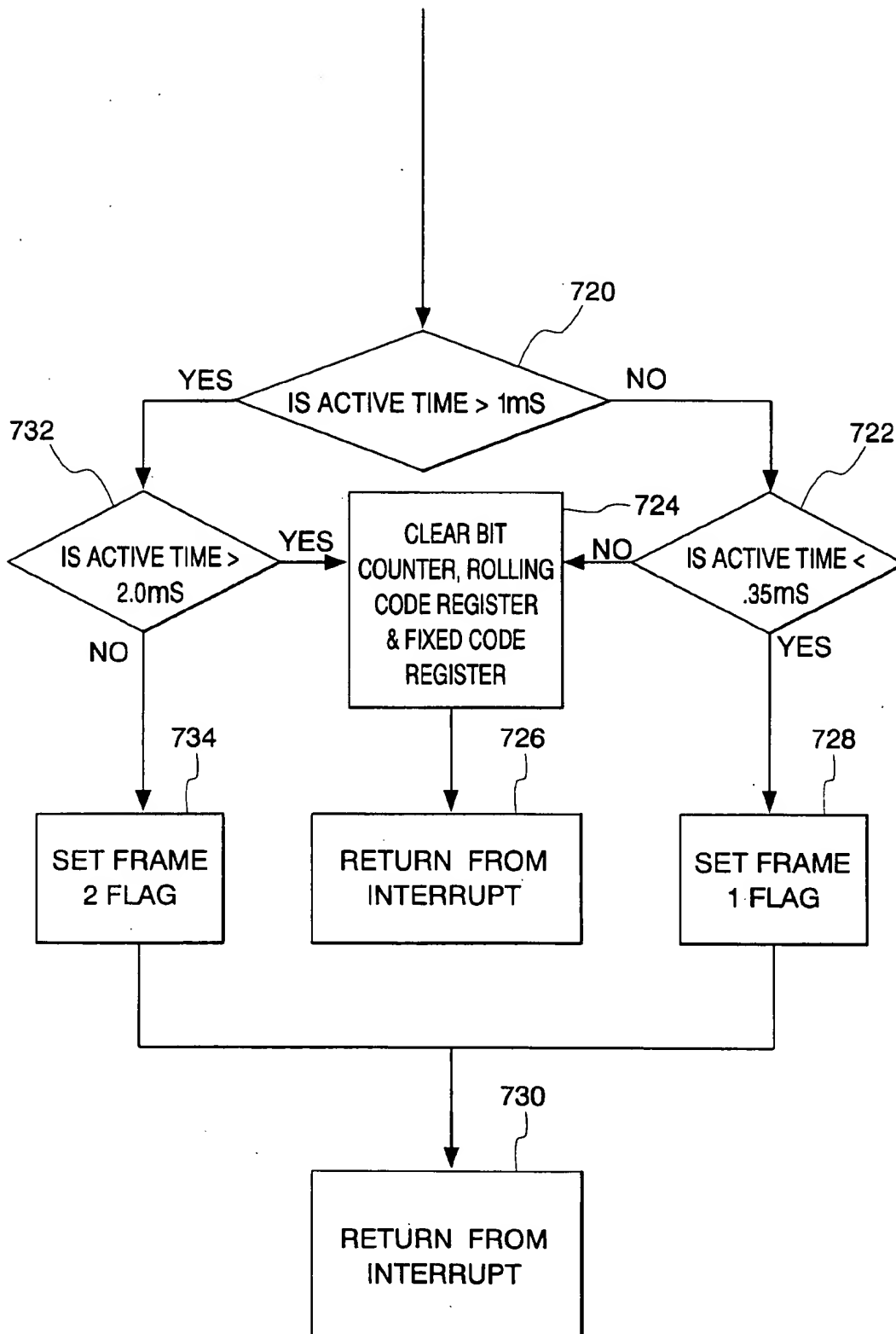
*Fig. 8C*

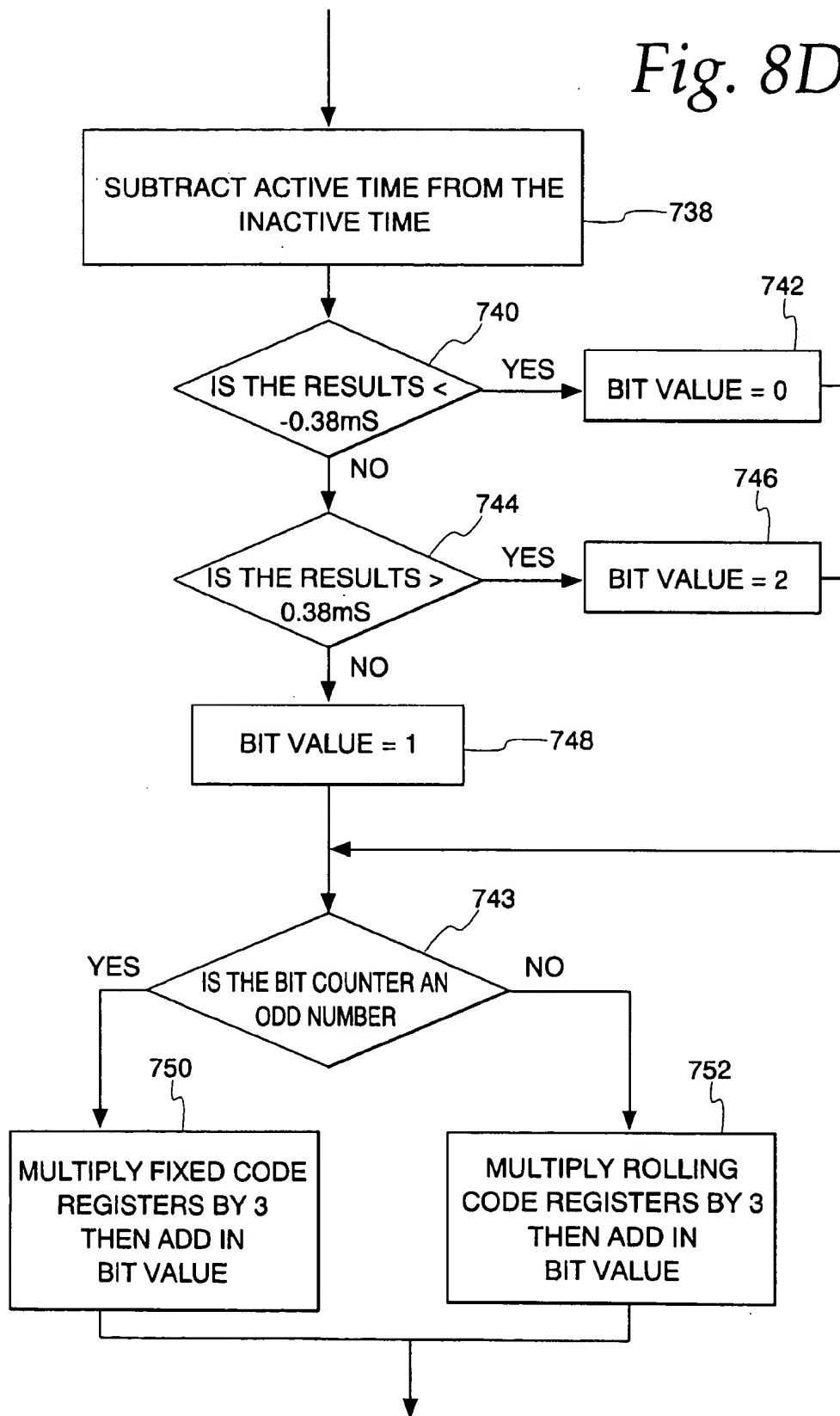
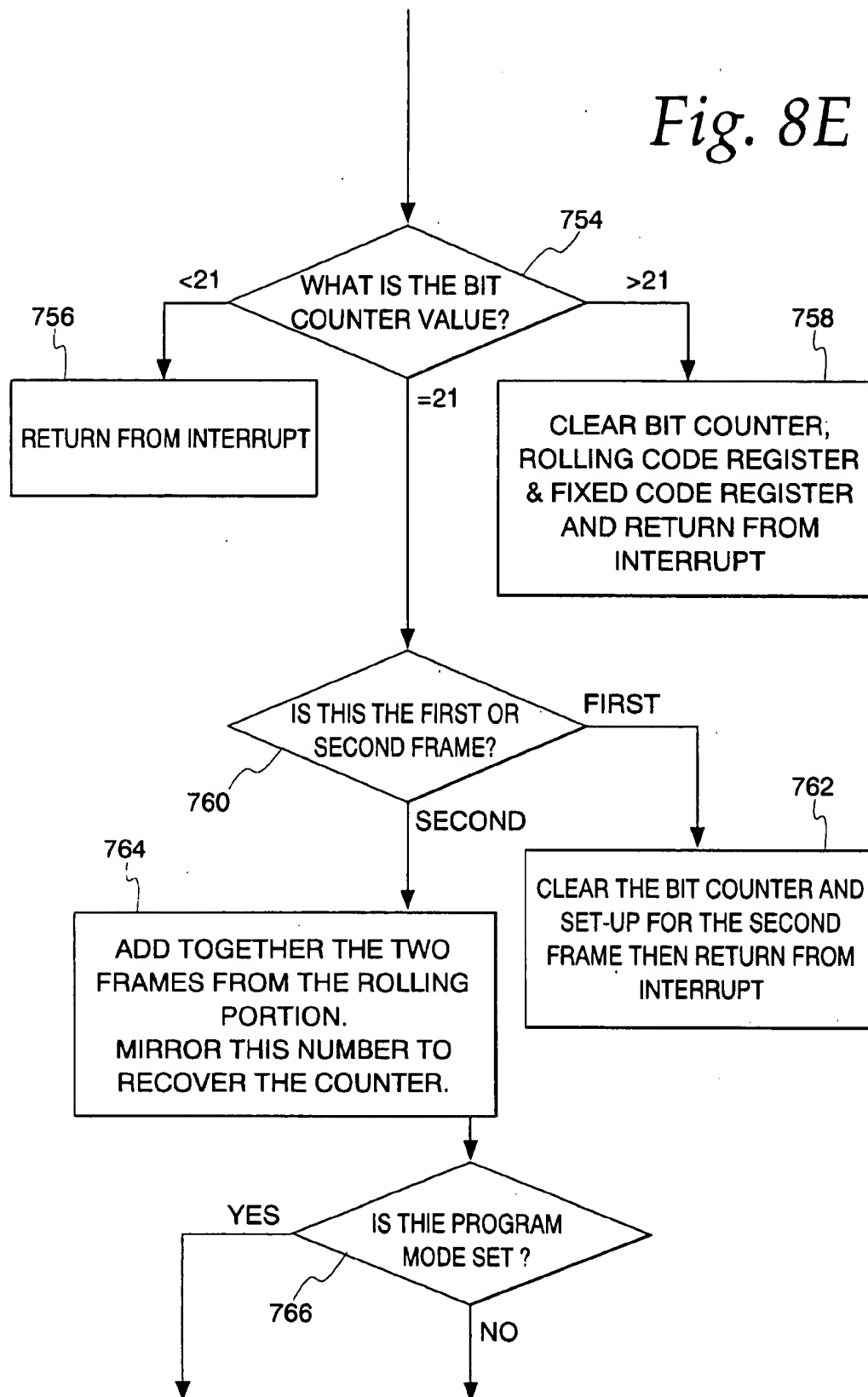
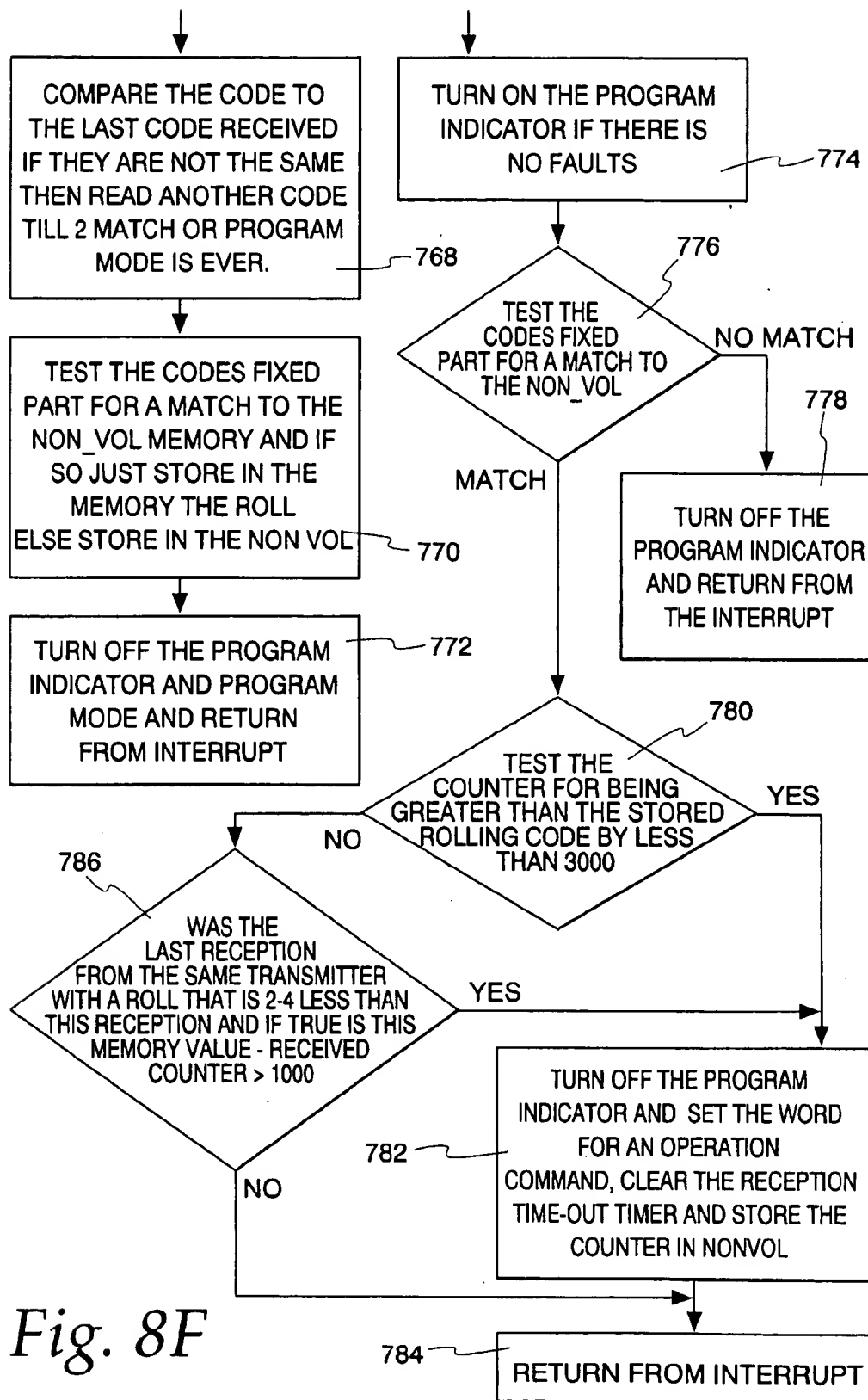
Fig. 8D

Fig. 8E

*Fig. 8F*

ROLLING CODE SECURITY SYSTEM

This application is a continuation, of application Ser. No. 08/446,886 filed May 17, 1995 now abandoned.

MICROFICHE APPENDIX

This application includes, pursuant to 37 C.F.R. 1.77(c) (2) and 37 C.F.R. 1.96(b), a microfiche appendix consisting of 1 sheet of microfiche containing 52 frames of an exemplary program listing of an exemplary embodiment of the present invention.

BACKGROUND OF THE INVENTION

The invention relates in general to security systems which allow operation upon the receipt of a properly coded signal. More particularly, the invention relates to a security system or to a barrier operator system, such as a garage door operator, employing a transmitter and a receiver which communicate via code streams having at least a portion thereof which changes with multiple operation of the device.

It is well known in the art to provide garage door operators or other barrier operators which include an electric motor connectable through a transmission to a door or other movable barrier which is to be opened and closed. Since many of these systems are associated with residences, as well as with garages, it is important that opening of the barrier be permitted only by one who is authorized to obtain entry to the area which the barrier protects. Some garage door operator systems have in the past employed mechanical lock and key arrangements associated with electrical switches mounted on the outside of the garage. While these systems enjoy a relatively high level of security, they are very inconvenient to use for a person because it necessitates them exiting their vehicle in order to send the command to open the garage door. This also may present some danger to people when the exit the relative security of their vehicle if someone may be waiting to do injury to them.

It is also well known to provide radio-controlled garage door operators which include a garage door operator unit having a radio receiver and a motor connected to be driven from the radio receiver. The radio receiver is adapted to receive radio frequency signals or other electromagnetic signals having particular signal characteristics which, when received, cause the door to be opened. More recently, such transmitter and receiver systems have become relatively more sophisticated in that they use radio transmitters which employ coded transmissions of multiple or three-valued digits, also known as "trinary bits" or other serial coded transmission techniques. Among these systems are U.S. Pat. No. 3,906,348 to Willmott, which employs a transmitter and receiver system wherein a plurality of mechanical switches may be used to set a stored authorization code.

U.S. Pat. No. 4,529,980 to Liotine et al. discloses a transmitter and receiver combination for use in a device such as a garage door operator wherein the transmitter stores an authorization code which is to be transmitted to and received by the receiver via a radio frequency link. In order to alter or update the authorization code contained within the transmitter, the receiver is equipped with a programming signal transmitter or light emitting diode which can send a digitized optical signal back to the transmitter where it is stored. Other systems also employing encoded transmissions are U.S. Pat. Nos. 4,037,201, 4,535,333, 4,638,433, 4,750,118 and 4,988,992.

While each of these devices have provided good security for the user, it is apparent that persons wishing to commit

property or person-related crimes have become more sophisticated as well. It is known in the security industry today that devices are being made available that can intercept or steal rolling code.

Transequalor Technology, Inc. sells integrated circuit code hopping encoders identified as KeeLoq Model NTQ105, NTQ115, NTQ125D and NTQ129. Some of the keeloq code hopping encoders generate serial codes having fixed portions, i.e., which do not change with repeated actuation of the encoding portion of the chip and rolling code portions which alter with each actuation of the encoding portion of the chip. In order to avoid, however, having the problem of the encoding portion of the chip having been inadvertently enabled and causing the rolling code to be altered on successive enabling attempts thereby leading to a rolling code which is transmitted and not recognized by a receiver, the keeloq code hopping encoders provide a window forward system, that is they are operable with systems having code receivers which recognize as a valid code not a single rolling code, but a plurality of rolling codes within a certain code window or window of values which are the values which would be generated on a relatively small number of switch closures as compared to the total number of rolling codes available. The problem with such a system, however, might arise if a user was away for a period of time or had inadvertently caused codes to be transmitted excluding the number of codes normally allowed within the valid forward code window. In that case, the rolling code would not be recognized by the receiver and the user could not gain entry without taking other measures to defeat the locking system or the garage door operator system which might involve the intervention of a trained engineer or technician.

Texas Instruments also has a prior system identified as the Mark Star TRC1300 and TRC1315 remote control transmitter/receiver combination. The system involves the use of a rolling code encoder which increments or rolls potentially the entire code, that is it does not leave a fixed portion. The system also includes a forward windowing function which allows an authorized user to be able to cause the receiver to be enabled within a limited number of key pushes. Like the keeloq system, if the forward window is exceeded, the Texas Instruments system must be placed in a learn mode to cause the system to relearn the code. In order to place the system into the learn mode, the person must obtain direct access to the receiver to cause a programming control system associated with the receiver to be hand actuated causing the receiver to enter a learn mode. Once the receiver has learned the new code, the receiver will then construct a new valid forward code window within which valid rolling codes may be received. The problem, of course, with such a system is that if, for instance in a garage door operator, the only portal of entry to the garage door is through the overhead door controlled by the garage door operator, the user will not be able to obtain entry to the garage without possibly having to do some damage to the structure. This problem is sometimes referred to in the industry as a "vaulted garage."

What is needed is an economical encoding system which provides good security by using a rolling code, but which enables a user of the system to proceed via a gradually degraded pathway in the event that the receiver detects a signal condition indicative of what might be a lack of security.

SUMMARY OF THE INVENTION

The invention relates in general to an electronic system for providing remote security for entry of actuation of a

particular device. Such a system may include a transmitter and receiver set, for instance with a hand-held transmitter and a receiver associated with a vehicle such as an automobile or the like. The transmitter, upon signaling the receiver, causing the vehicle to start up or to perform other functions. The system may also be useful in a barrier operator system such as a garage door operator by allowing the garage door to be opened and closed in a relatively secure fashion while preventing persons who may be intercepting the radio frequency signals from being able to, although unauthorized, cause the vehicle to begin running or to allow access to the garage.

Hopping: Fix
rolling
The system includes a transmitter generally having means for developing a fixed code and a rolling or variable code. The rolling or variable code is changed with each actuation of the transmitter. The fixed code remains the same for each actuation of the transmitter. In the present system, the transmitter includes means for producing a 32-bit frame comprising the fixed portion of the code and a second 32-bit frame comprising the variable portion of the code. The 32-bit rolling code is then mirrored to provide a 32-bit mirrored rolling code. The 32-bit mirrored rolling code then has its most significant bit "deleted" by setting it to zero. The transmitter then converts the 32-bit fixed code and the mirrored variable code to a three-valued or trinary bit fixed code and a three-valued or trinary bit variable code or rolling code.

demodulated
To provide further security, the fixed code and the rolling codes are shuffled so that alternating trinary bits are comprised of a fixed code bit and a rolling code bit to yield a total of 40 trinary bits. The 40 trinary bits are then packaged in a first 20-trinary bit frame and a second 20-trinary bit frame which have proceeding them a single synchronization and/or identification pulse indicating the start of the frame and whether it is the first frame or the second frame. Immediately following each of the frames, the transmitter is placed into a quieting condition to maintain the average power of the transmitter over a typical 100 millisecond interval within legal limits promulgated by the United States Federal Communications Commission. The first trinary frame and the second trinary frame are used to modulate a radio frequency carrier, in this case via amplitude modulation to produce an amplitude modulated encrypted signal. In a preferred embodiment, the radio frequency signal is amplitude modulated. The amplitude modulated signal is then launched and may be received by an AM receiver. In the preferred embodiment, the AM receiver receives the amplitude modulated signal, demodulates it to produce a pair of trinary bit encoded frames. The trinary bits in each of the frames are converted on the fly to 2-bit or half nibbles indicative of the values of the trinary bits which are ultimately used to form two 16-bit fixed code words and two 16-bit variable code words. The two 16-bit fixed code words are used as a pointer to identify the location of a previously stored rolling code value within the receiver. The two 16-bit rolling code words are concatenated by taking the 16-bit word having the more significant bits, multiplying it by 310 and then adding it to the second of the words to produce a 32-bit encrypted rolling code. In order to make certain that if the transmitter was inadvertently actuated a number of times, the authorized user can still start his car or gain entry to his garage. The 32-bit encrypted code is then compared via a binary subtraction with the stored rolling code. If the 32-bit code is within a window or fixed count, in the present embodiment 1000, the microprocessor produces an authorization signal which is then responded to by other portions of the circuit to cause the garage door to open or close as commanded. In the

event that the code is greater than the stored rolling code, plus 1000, indicative of a relatively large number of incrementations, the user is not locked out of the garage, but is allowed to provide further signals or indicia to the receiver that he is an authorized user without any significant degradation of the security. This is done by the receiver entering an alternate mode requiring two or more successive valid codes to be received, rather than just one. If the two or more successive valid codes are received, the garage door will open. However, in order to prevent a person who has previously or recently recorded a recent valid code from being able to obtain access to the garage, a trailing window, in this case starting at a count of 300 less than the present stored count and including all code values between the present stored count and 300 less is compared to the received code. If the received code is within this backward window, the response of the system simply is to take no further action, nor to provide authorization during that code cycle on the assumption that the code has been purloined.

Thus, the present system provides important advantages over the previous garage door operator systems and even previous rolling code systems. The system provides a multiple segmented windowed system which provides a valid code window, a second relatively insecure code window in which two successive valid codes must be received and finally a window in which no valid codes are recognized due to the likelihood of the receiver having been stolen.

It is a principal object of the present invention to provide a security system involving a radio frequency transmitter and receiver wherein multiple security conditions may exist requiring different levels of signal security.

It is another object of the present invention to provide a secure radio transmitter receiver system which may rapidly and easily decode a relatively large code combination.

Other advantages of the invention will become obvious to one of ordinary skill in the art upon a perusal of the following specification and claims in light of the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a perspective view of an apparatus for moving a barrier or garage embodying the present invention;

FIG. 2 is a block diagram of a transmitter for use with a garage door operator of FIG. 1;

FIG. 3 is a block diagram of a receiver positioned within a head unit of the garage door operator shown in FIG. 1;

FIG. 4 is a schematic diagram of the transmitter shown in FIG. 2;

FIGS. 5A-B is a schematic diagram of the receiver shown in FIG. 3;

FIG. 6 is a timing diagram of signals generated by a portion of the transmitter;

FIGS. 7A, B, and C are flow diagrams showing the operation of the transmitter; and

FIGS. 8A, B, C, D, E and F are flow charts showing the operation of the receiver.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Referring now to the drawings and especially to FIG. 1, more specifically a movable barrier door operator or garage door operator is generally shown therein and includes a head unit 12 mounted within a garage 14. More specifically, the head unit 12 is mounted to the ceiling of the garage 14 and

includes a rail 18 extending therefrom with a releasable trolley 20 attached having an arm 22 extending to a multiple paneled garage door 24 positioned for movement along a pair of door rails 26 and 28. The system includes a hand-held transmitter unit 30 adapted to send signals to an antenna 32 positioned on the head unit 12 and coupled to a receiver as will appear hereinafter. An external control pad 34 is positioned on the outside of the garage having a plurality of buttons thereon and communicate via radio frequency transmission with the antenna 32 of the head unit 12.

An optical emitter 42 is connected via a power and signal line 44 to the head unit. An optical detector 46 is connected via a wire 48 to the head unit 12.

Referring now to FIG. 2, the transmitter 30 is shown therein in general and includes a battery 70 connected by a pushbutton switch 72 to a power supply 74 which is coupled via leads 75 and 76 to a microcontroller 78. The microcontroller 78 is connected by a serial bus 79 to a non-volatile memory 80. An output bus 81 connects the microcontroller to a radio frequency oscillator 82. The microcontroller 78 produces coded signals when the button 72 is pushed causing the output of the RF oscillator 82 to be amplitude modulated to supply a radio frequency signal at an antenna 83 connected thereto. More specifically, as shown in FIG. 4, details of the transmitter 30 are shown therein, including a plurality of switches 72. When switch 72 is closed, power is supplied through a diode 100 to a capacitor 102 to supply a 7.1 volt voltage at a lead 103 connected thereto. A light emitting diode 104 indicates that the transmitter button has been pushed and provides a voltage to a lead 105 connected thereto. A Zener diode 106 provides voltage regulation and causes the back biased diode 107 to cause the crystal 108 to be energized, thereby energizing the microcontroller 78, a Zilog 125C0113 8-bit microcontroller in this embodiment. The signal is also sent via a resistor 110 through a lead 111 to a P32 pin of the microcontroller 78. Likewise, when a switch 113 is closed, current is fed through a diode 114 to the lead 103 also causing the crystal 108 to be energized, powering up the microcontroller at the same time that pin P33 of the microcontroller is pulled up. Similarly, when a switch 118 is closed, power is fed through a diode 119 to the crystal 108 as well as pull up voltage being provided through a resistor 120 to the pin P31. It should also be appreciated that pin P34 of the microcontroller is configured via a connection with the resistor 123 to be an RS232 input port 124.

The microcontroller is coupled via the serial bus 79 to a chip select port, a clock port and a DI port to which and from which serial data may be written and read and to which addresses may be applied. As will be seen hereinafter in the operation of the microcontroller, the microcontroller 78 produces output signals at the lead 81, which are supplied to a resistor 125 which is coupled to a voltage dividing resistor 126 feeding signals to the lead 127. A 30-nanohenry inductor 128 is coupled to an NPN transistor 129 at its base 130. The transistor 129 has a collector 131 and an emitter 132. The collector 131 is connected to the antenna 83 which, in this case, comprises a printed circuit board, loop antenna having an inductance of 25-nanohenries, comprising a portion of the tank circuit with a capacitor 133, a variable capacitor 134 for tuning, a capacitor 135 and a capacitor 136. An 30-nanohenry inductor 138 is coupled via a capacitor 139 to ground. The capacitor has a resistor 140 connected in parallel with it to ground. When the output from lead 81 is driven high by the microcontroller, the transistor Q1 is switched on causing the tank circuit to output a signal on the antenna 83. When the transistor Q1 is switched off, the

output to the drive the tank circuit is extinguished causing the radio frequency signal at the antenna 83 also to be extinguished.

Referring now to FIG. 3, the receiver is shown therein and includes a receiver antenna 200 coupled to an amplitude modulated receiver 202 driven from a power supply 204 connectable to a source of alternating current 206. The receiver 202 provides a demodulated output via a bandpass filter 210 to an analog-to-digital converter 212 which provides input to a microcontroller 214 having an internal read-only memory 216 and an internal random-access memory 218. A serial non-volatile memory 220 is connected via a memory bus 222 to the microcontroller 214 to send and receive information thereto. The microcontroller has an output line 226 coupled to a motor controller 228 which may include a plurality of relays or other standard electromechanical features which feeds electrical current on lines 230 and 232 to an electric motor 234.

Referring now to FIGS. 5A-B the antenna 200 coupled to a reactive divider network 250 comprised of a pair of series connected inductances 252 and 254 and capacitors 256 and 258 which supply an RF signal to a buffer amplifier having an NPN transistor 260, at its emitter 261. The NPN transistor 260 has a pair of capacitors 262 and 264 connected to it for power supply isolation. The buffer amplifier provides a buffered radio frequency output signal on a lead 268. The buffered RF signal is fed to an input 270 which forms part of a super-regenerative receiver 272 having an output at a line 274 coupled to the bandpass filter which provides digital output to the bandpass filter 212. The bandpass filter 212 includes a first stage 276 and a second stage 278 to provide a digital level output signal at a lead 280 which is supplied via an averaging circuit 282 to an input pin P32 of the microcontroller 214.

The microcontroller 214 may have its mode of operation controlled by a programming or learning switch 300 coupled via a line 302 to the P25 pin. A command switch 304 is coupled via a jumper 306 to a line 308 and ultimately through a resistor to the input pin P22. A pin P21 sinks current through a resistor 314 connected to a light emitting diode 316, causing the diode to light to indicate that the receiver is active. The microcontroller 214 has a 4 MHz crystal 328 connected to it to provide clock signals and includes an RS232 output port 332 that is coupled to the pin P31. A switch 340 selects whether constant pressure or monostable is to be selected as the output from output terminals P24 and P23 which are coupled to a transistor 350 which, when switched on, sinks current through a coil 352 of a relay 354, causing the relay to close to provide an actuating signal on a pair of leads 356 and 358 to an electric motor.

It may be appreciated that the power supply 204 may receive power from an external transformer or other AC source through a jack 370 which is connected to a pair of RJ uncoupling capacitors 372 and 374. The input signal is then set to a full-wave rectifier bridge 376 which provides an output current at a resistor 378. An 18-volt Zener diode 380 is connected between ground and the resistor 378 and includes high frequency bypass capacitor 382 connected in parallel with it. An 8.2-volt Zener diode 384 is connected in back-biased configuration to the resistor 378 to receive a signal therefrom to guarantee that at least an 8.2-volt signal is fed to a resistor 390 causing an LED 392 to be illuminated and also causing power to be supplied to a 5-volt 78L05 voltage regulator 396. The voltage regulator 396 supplies regulated voltage to an output line 398. Filtering capacitors 400a, 400b, 400c and 400d limit the fluctuations at the power supply.

The program code listing for the transmitter is set forth at pages A-1 through A-19 and for the receiver at pages A-20 through A-50 of the microfiche appendix. Referring now to FIGS. 7A through 7C, the flow chart set forth therein describes the operation of the transmitter. A rolling code is incremented by three in a step 500, followed by the rolling code being stored for the next transmission from the transmitter when the transmitter button is pushed. The order of the binary digits in the rolling code is inverted or mirrored in a step 504, following which in a step 506, the most significant digit is converted to zero effectively truncating the binary rolling code. The rolling code is then changed to a trinary code having values 0, 1 and 2 and the initial trinary rolling code is set to 0. It may be appreciated that it is trinary code which is actually used to modify the radio frequency oscillator signal and the trinary code is best seen in FIG. 6. It may be noted that the bit timing in FIG. 6 for a 0 is 1.5 milliseconds down time and 0.5 millisecond up time, for a 1, 1 millisecond down and 1 millisecond up and for a 2, 0.5 millisecond down and 1.5 milliseconds up. The up time is actually the active time when carrier is being generated. The down time is inactive when the carrier is cut off. The codes are assembled in two frames, each of 20 trinary bits, with the first frame being identified by a 0.5 millisecond sync bit and the second frame being identified by a 1.5 millisecond sync bit.

In a step 510, the next highest power of 3 is subtracted from the rolling code and a test is made in a step 512 to determine if the result is equal to zero. If it is, the next most significant digit of the binary rolling code is incremented in a step 514, following which flow is returned to the step 510. If the result is not greater than 0, the next highest power of 3 is added to the rolling code in the step 516. In the step 518, another highest power of 3 is incremented and in a step 520, a test is determined as to whether the rolling code is completed. If it is not, control is transferred back to step 510. If it has, control is transferred to step 522 to clear the bit counter. In a step 524, the blank timer is tested to determine whether it is active or not. If it is not, a test is made in a step 526 to determine whether the blank time has expired. If the blank time has not expired, control is transferred to a step 528 in which the bit counter is incremented, following which control is transferred back to the decision step 524. If the blank time has expired as measured in decision step 526, the blank timer is stopped in a step 530 and the bit counter is incremented in a step 532. The bit counter is then tested for odd or even in a step 534. If the bit counter is not even, control is transferred to a step 536 where the output bit of the bit counter divided by 2 is fixed. If the bit counter is even, the output bit counter divided by 2 is rolling in a step 538. The bit counter is tested to determine whether it is set to equal to 80 in a step 540. If it is, the blank timer is started in a step 542. If it is not, the bit counter is tested for whether it is equal to 40 in a step 544. If it is, the blank timer is tested and is started in a step 544. If the bit counter is not equal to 40, control is transferred back to step 522.

Referring now to FIGS. 8A through 8F and, in particular, to FIG. 8A, the operation of the receiver is set forth therein. In a step 700, an interrupt is detected and acted upon from the radio input pin. The time difference between the last edge is determined and the radio inactive timer is cleared in step 702. A determination is made as to whether this is an active time or inactive time in a step 704, i.e., whether the signal is being sent with carrier or not. If it is an inactive time, indicating the absence of carrier, control is transferred to a step 706 to store the inactive time in the memory and the routine is exited in a step 708. In the event that it is an active

time, the active time is stored in memory in a step 710 and the bit center is tested in a step 712. If the bit counter zero, control is transferred to a step 714, as may best be seen in FIG. 8B and a test is made to determine whether the inactive time is between 20 milliseconds and 55 milliseconds. If it is not, the bit counter is cleared as well as the rolling code register and the fixed code register in step 716 and the routine is exited in step 718.

In the event that the inactive time is between 20 milliseconds and 55 milliseconds, a test is made in a step 720 to determine whether the active time is greater than 1 millisecond, as shown in FIG. 8C. If it is not, a test is made in a step 722 to determine whether the inactive time is less than 0.35 millisecond. If it is, a frame 1 flag is set in a step 728 identifying the incoming information as being associated with frame 1 and the interrupt routine is exited in a step 730. In the event that the active time test in step 722 is not less than 0.35 millisecond, in the step 724, the bit counter is cleared as well as the rolling code register and the fixed register and the return is exited in the step 726. If the active time is greater than 1 millisecond as tested in step 720, a test is made in a step 732 to determine whether the active time is greater than 2.0 milliseconds. If it is not, the frame 2 flag is set in a step 734 and the routine is exited in step 730. If the active time is greater than 2 milliseconds, the bit counter rolling code register and fixed code register are cleared in step 724 and the routine is exited in step 726.

In the event that the bit counter test in step 712 indicates that the bit counter is not 0, control is transferred to step 736, as shown in FIG. 8A. Both the active and inactive periods are tested to determine whether they are less than 4.5 milliseconds. If either is not less than 4.5 milliseconds, the bit counter is cleared as well as the rolling code register and the fixed code registers. If both are equal to greater than 4.5 milliseconds, the bit counter is incremented and the active time is subtracted from the inactive time in the step 738, as shown in FIG. 8D. In the step 740, the results of the subtraction are determined as to whether they are less than 0.38 milliseconds. If they are, the bit value is set equal to zero in step 742 and control is transferred to a decision step 743. If the results are not less than 0.38 milliseconds, a test is made in a step 744 to determine if they difference between the active time and inactive time is greater than 0.38 milliseconds and control is then transferred to a step 746 setting the bit value equal to 2. Both of the bit values being set in steps 742 and 746 relate to a translation from the three-level trinary bits 0, 1 and 2 to a binary number.

If the result of the step 744 is in the negative, the bit value is set equal to 1 in step 748. Control is then transferred to the step 743 to test whether the bit counter is set to an odd or an even number. If it is set to an odd number, control is transferred to a step 750 where the fixed code, indicative of the fact that the bit is an odd numbered bit in the frame sequence, rather an even numbered bit, which would imply that it is one of the interleaved rolling code bits, is multiplied by three and then the bit value added in.

If the bit counter indicates that it is an odd number trinary bit being processed, the existing rolling code registers are multiplied by three and then the trinary bit value obtained from steps 742, 746 and 748 is added in. Whether step 750 or 752 occurs, the bit counter value is the tested in the step 754, as shown in FIG. 8E. If the bit counter value is greater than 21, the bit counter rolling code register and fixed code register are cleared in the step 758 and the routine is exited. If the bit counter value is less than 21, there is a return from the interrupt sequence in a step 756. If the bit counter value is equal to 21, indicating that a sink bit plus trinary data bits

have been received, a test is made in a step 760 to determine whether the sink bit was indicative of a first or second frame, if it was indicative of a first frame, the bit counter is cleared and set up is done for the second frame following which there is a return from the routine in the step 762. In the event that the second frame is indicated as being received by the decision of step 760, the two frames have their rolling contributions added together to form the complete inverted rolling code. The rolling code is then inverted or mirrored to recover the rolling code counter value in the step 764. A test is made in the step 766 to determine whether the program mode has been set. If it has been set, control is transferred to a step 768 where the code is compared to the last code received. If there is no match, as would be needed in order to get programming, then another code will be read until two successive codes match or the program mode is terminated. In a step 770, the codes are tested such that the fixed codes are tested for a match with a fixed code in non-volatile memory. If there is a match, the rolling portion is stored in the memory. If there is not, it is stored in the non-volatile memory. Control is then transferred to step 772, the program indicator is switched off, the program mode is exited and there is a return from the interrupt. In the event that the test of step 766 indicates that the program mode has not been set, the program indicator is switched on in a step 774, as shown in FIG. 8F. The codes are tested to determine whether there is a match for the fixed portion of the code in the step 776. If there is no match, the program indicator is switched off and the routine is exited in step 778. If there is a match, the counter which is indicative of the rolling code is tested to determine whether its value is greater than the stored rolling code by a factor or difference of less than 3,000 indicating an interval of 1,000 button pushes for the transmitter. If it is not, a test is made in the step 786 to determine whether the last transmission from the same transmitter is with a rolling code that is two to four less than the reception and, if true, is the memory value minus the received rolling code counter value greater than 1,000. If it is, control is transferred to a step 782 switching off the program indicator and setting the operation command word causing a commanded signal to operate the garage door operator. The reception time out timer is cleared and the counter value for the rolling code is stored in non-volatile memory, following which the routine is exited in the step 784. In the event that the difference is not greater than 1,000, in step 786 there is an immediate return from the interrupt in the step 784. In the event that the counter test in the step 780 is positive, steps 782 and 784 are then executed thereafter.

While there has been illustrated and described a particular embodiment of the present invention, it will be appreciated that numerous changes and modifications will occur to those skilled in the art, and it is intended in the appended claims to cover all those changes and modifications which fall within the true spirit and scope of the present invention.

What is claimed is:

1. A transmitter for sending an encrypted signal to control an actuator, comprising:

oscillator for generating a radio frequency oscillatory signal;

apparatus for enabling the sending of an encrypted signal; binary code generator responsive to the enabling apparatus for generating a variable binary code, said variable code being different for each enabling by the enabling device;

trinary code generator for generating a three-valued or trinary code responsive to the variable binary code; and

transmitting apparatus for modulating the radio frequency oscillatory signal with the trinary code to produce a modulated trinary coded variable radio frequency signal for operation or control of a secure actuator.

2. A transmitter for sending an encrypted signal to control an actuator according to claim 1, further comprising apparatus for receiving said variable binary signal and producing a mirrored binary signal, said mirrored binary signal being supplied to said trinary code generator for generating the trinary signal from the variable binary signal.

3. A transmitter for sending an encrypted signal to control an actuator according to claim 1, comprising apparatus for producing a fixed code signal and for combining said fixed code signal with a rolling code signal.

4. A transmitter for sending an encrypted signal to control an actuator according to claim 3, comprising apparatus for interleaving trinary bits derived from said fixed code signal with trinary bits derived from said rolling code signal to produce a trinary interleaved fixed and rolling code signal.

5. A transmitter for sending an encrypted signal to control an actuator according to claim 1, comprising incrementing apparatus for altering said variable code by adding a fixed value with each enabling apparatus actuation.

6. A transmitter for sending an encrypted signal to control an actuator according to claim 5, wherein said means for incrementing said variable code increments said variable code by a prime number value.

7. A transmitter for sending an encrypted signal to control an actuator according to claim 1, wherein said binary code generator for generating a variable binary code includes a non-volatile memory for storing a variable binary code.

8. A transmitter for sending an encrypted signal to control an actuator according to claim 1, wherein said binary code generator for generating said variable code includes storage means holding a previous cycle variable code signal from which the variable code is generated.

9. A remote security system for communicating an encrypted signal to a control actuator, comprising:

binary code generator for generating a sequence of variable binary codes according to a predetermined algorithm, successive codes in the sequence being different from preceding codes in the sequence;

trinary code generator for converting said generated variable binary code to a trinary code;

a transmitter for modulating a transmitted radio frequency signal with said trinary code;

a radio-frequency receiver for demodulating said transmitted modulated radio frequency signal and providing a received trinary code;

trinary code convertor for converting said received trinary code to a received binary code;

a controller responsive to a positive comparison of said received binary code and a reference variable binary code; and

update apparatus responsive to said positive comparison for updating said reference variable binary code according to said received binary code.

10. A remote security system according to claim 9, wherein said update apparatus updates said reference variable binary code by performing said predetermined algorithm on said reference variable binary code.

11. A remote security system according to claim 9, wherein said positive comparison results if said received binary code and said reference variable binary code lie within a predetermined numerical limit of one another.

12. A remote security system according to claim 11, wherein said positive comparison results if the numerical

11

difference of said received binary code minus said reference variable binary code is a positive number less than said predetermined limit.

13. A remote security system according to claim 12, wherein said predetermined limit is about 1000.

14. A remote security system according to claim 12, wherein said positive comparison results if at least two said received binary codes transmitted in succession, each of which is numerically different from said reference variable binary code by a number outside the range of said predetermined limit, represent successive results of said predetermined algorithm.

15. A remote security system according to claim 14, wherein said positive comparison results if said successively transmitted codes which represent successive results of said preselected algorithm, each yield a difference when subtracted from said reference variable binary code outside the range of zero to a second predetermined limit.

16. A remote security system according to claim 15, wherein said second predetermined limit is about 300.

17. A remote security system according to claim 11, wherein the variable binary code is a rolling code and the system further comprises a binary code combiner for combining a binary fixed code with said binary rolling code and providing the combination to said trinary code generator.

18. A remote security system according to claim 17, further comprising apparatus for interleaving trinary bits derived from said binary fixed code with trinary bits derived from said binary rolling code to provide an interleaved trinary fixed-and-rolling code to said transmitter.

19. A remote security system according to claim 18, further comprising apparatus for receiving said output of

12

said radio-frequency receiver and separating said interleaved fixed-and-rolling code and providing to said trinary code convertor a received trinary fixed code and a received trinary rolling code.

20. A remote security system according to claim 19, wherein said trinary code convertor provides a received binary fixed code in response to said received trinary fixed code and a received binary rolling code in response to said received trinary rolling code, and further comprising addressing apparatus for using said received binary fixed code to address said reference variable binary code in a memory.

21. A remote security system according to claim 20, further comprising means for mirroring said binary rolling code and providing it to said trinary code generator.

22. A remote security system according to claim 21, further comprising apparatus for mirroring said received binary rolling code and providing it to said controller and to said update apparatus.

23. A remote security system according to claim 22, wherein said predetermined algorithm generates a variable binary code by adding a numeric constant to it.

24. A remote security system according to claim 23, wherein said predetermined algorithm generates a variable binary code by adding the value 3 to it.

25. A remote security system according to claim 15, further comprising second update apparatus for updating said reference variable binary code according to one of the set of said successively transmitted received binary codes.

* * * * *